

IET Cyber-Physical Systems: Theory & Applications

Special issue Call for Papers

**Be Seen. Be Cited.
Submit your work to a new
IET special issue**

Connect with researchers and
experts in your field and share
knowledge.

Be part of the latest research
trends, faster.

Read more



The Institution of
Engineering and Technology



REVIEW

A review: Monitoring situational awareness of smart grid cyber-physical systems and critical asset identification

Yazeed Alrowaili¹  | Neetesh Saxena¹  | Anurag Srivastava² | Mauro Conti³ | Pete Burnap¹

¹School of Computer Science and Informatics, Cardiff University, Cardiff, UK

²Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, West Virginia, USA

³Department of Mathematics, University of Padua, Padua, Italy

Correspondence

Yazeed Alrowaili and Neetesh Saxena.
Email: AlrowailiYT@cardiff.ac.uk and Saxenan4@cardiff.ac.uk

Abstract

Cyber-Physical Systems (CPSs) are becoming more automated and aimed to be as efficient as possible by enabling integration between their operations and Information Technology (IT) resources. In combination with production automation, these systems need to identify their assets and the correlation between them; any potential threats or failures alert the relevant user/department and suggest the appropriate remediation plan. Moreover, identifying critical assets in these systems is essential. With numerous research and technologies available, assessing IT assets nowadays can be straightforward to implement. However, there is one significant issue of evaluating operational technology critical assets since they have different characteristics, and traditional solutions cannot work efficiently. This study presents the necessary background to attain the appropriate approach for monitoring critical assets in CPSs' Situational Awareness (SA). Additionally, the study presents a broad survey supported by an in-depth review of previous works in three important aspects. First, it reviews the applicability of possible techniques, tools and solutions that can be used to collect detailed information from such systems. Secondly, it covers studies that were implemented to evaluate the criticality of assets in CPSs, demonstrates requirements for critical asset identification, explores different risks and failure techniques utilised in these systems and delves into approaches to evaluate such methods in energy systems. Finally, this paper highlights and analyses SA gaps based on existing solutions, provides future directions and discusses open research issues.

KEYWORDS

critical infrastructures, cyber-physical systems

1 | INTRODUCTION

Failure to secure or operate Cyber-Physical Systems (CPSs) is not tolerated. It can lead to serious complications, such as severe injuries to people and massive losses of equipment, properties and even cities linked to these systems [1]. Nevertheless, such systems need to have a highly secure and dependable communication network that offers a mutual flow of communicated information that can help create automated and distributed procedures. The cybersecurity of such systems is significantly crucial since several Internet of Things devices operating on different network technologies are connected to

these systems. In this way, a wide communication network surface increases the number of cyber threats that can occur in the system [2]. This could be because CPSs are moving from being stand-alone and isolated systems to systems that can have two-way communication to create automated and distributed procedures that can help increase productivity. The integration makes such systems target cybersecurity attacks like traditional Information Technology (IT). Therefore, monitoring and advancing Situational Awareness (SA) in such systems are substantially vital. The examination can help gather information from IT and Operational Technology (OT) resources and physical access systems in cyber-physical

This is an open access article under the terms of the [Creative Commons Attribution](https://creativecommons.org/licenses/by/4.0/) License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2023 The Authors. *IET Cyber-Physical Systems: Theory & Applications* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

structures. Then, the information collected can be analysed to identify problems inside these systems before they occur, providing comprehensive knowledge about the system and helping to build advanced alert capabilities.

To begin with, one of the various types of CPSs is energy systems. Moreover, these systems are considered extremely critical for two reasons: (1) any cyber incidents that happen on these systems can directly affect the safety of human life and (2) the cyber threats on these systems can affect the utility and/or a nation from an economic perspective.

Motivation. We highlight a few cyber threats case studies that occurred on different CPSs, which show why protecting them is essential. Musleh et al. [3] discussed significant cyberattacks that occurred in the energy sector. In 2007, in Idaho, USA, an exploded generator caused by an Aurora attack manipulated a circuit breaker of a diesel generator. In Turkey, in 2008, 30,000 barrels of oil spilled into the water after an explosion occurred due to an attack that manipulated the control system parameters of an oil pipeline. In 2012, in Saudi Arabia, the generation and delivery of energy were severely affected by a malware injection that targeted the Aramco company. As we can observe from the previous case studies, securing such systems is paramount. These systems are not just regular systems but can be considered a backbone for a nation's economy. The increase in cyber threats that target these systems have raised these concerns. Likewise, in 2015, a cyberattack in Ukraine targeted three distribution substations due to unauthorised entry into the company's Supervisory Control and Data Acquisition (SCADA) system. This attack was highly severe because it caused a blackout affecting 225,000 customers for several hours in 103 cities [4]. Therefore, a cybersecurity threat on these systems can continue to affect the economy and many lives. Lastly, another recent incident in 2021 was about an attacker gaining unauthorised access to the Human–Machine Interface (HMI) located in a Florida water treatment plant. Moreover, the attacker tried to adjust the sodium hydroxide level from 100 ppm to 11,100 ppm, easily affecting human life falling under the attacked water supply network [5]. To conclude, these systems need the appropriate mechanisms to capture and analyse real-time data through SA, identify visible and invisible attacks and apply the best remediation plan.

Context. In this study, we consider energy systems as a case study. Currently, the energy sectors use Smart Grids (SGs) as one of their energy resources through electricity. The SG systems have critical procedures to generate, transmit and distribute energy, offer a mutual flow of electricity and provide information that can help create automated and distributed energy delivery networks [6]. Moreover, SGs use two-way communication in all their processes, from generation to distribution, providing numerous advantages to both consumers/producers. Nevertheless, procedures performed on these systems need to be monitored and controlled by devices specially designed for Industrial Control Systems (ICSs). Colbert and Kott [7] define ICSs as a set of various control systems and equipment that contain hardware,

software and networks that operate and automate industrial processes. Still, the primary security goals in both OT and IT are not the same; OT devices are time-critical. The primary security goal of such a system is to provide availability at any time when needed. Therefore, SG systems are considered CPSs, and there is a high demand to secure such systems to avoid any adverse human or economic consequences. Furthermore, in this study, we mainly covered survey papers that delve into tools, techniques and simulations applied to the SG. These papers focus on asset discovery, identification of cybersecurity issues, and assessment of risks and failures where the impact on power components (physical assets) is illustrated. These points are highly relevant to the aim of our paper. We have explored journal articles, peer-reviewed international conferences, security blogs and books to refine and refer our work to offer constructive arguments. We are aware that there are additional studies conducted on other CPSs, such as oil and gas, and transportation network systems. However, due to the different physical functionalities and requirements within these CPSs, these studies are considered outside the scope of this study.

Challenges. Cyber-Physical Systems are considered different from other traditional systems because CPSs utilise ICS to perform specific operational and industrial physical tasks. These systems have attracted the attention of adversaries due to the high frequency of targeted cyber threats. Furthermore, monitoring such systems for any cyber threats has numerous challenges. One of the significant challenges in such a system is that the ICS assets are different from any IT assets, making them hard to deal with, secure, explore and identify. Moreover, some of these assets are considered legacy systems that can be incredibly difficult to deal with regarding security; for instance, Programmable Logic Controllers (PLCs), Intelligent Electronic Devices (IEDs) or even sensors can be undetectable because these assets are so out of date [8]. Another challenge is that these assets are time-critical with a limited process and have specified communication techniques, making them highly sensitive to any exploring technique (passive, active or hybrid). Unlike traditional IT assets, any unnecessary usage of the discovery tool can affect the entire system's performance [9].

It is also essential to classify all identified assets based on their criticality. Such classification is needed since a CPS is built to satisfy a specific need. The assets in SG systems have their characteristics. For example, one of the different assets of SGs is transformers, which transform voltage into either step-up/step-down, and the failure to protect such an asset is not tolerated [10]. A further challenge is that it is vital to identify all possible cyber threats in such a system. Furthermore, the identified threats should be classified based on the assets' criticality, which must be handled immediately. For instance, targeting a critical asset with a simple attack should not be acceptable at all [11]. Such a system needs complete knowledge about the entire procedures, devices, users, resources and policies, which can be used to build the advanced alert capability. Moreover, it is challenging to have massive data from different systems analysed using different approaches.

Analysing data and indicators from different sources can highly enhance the SA of these systems that can better build a system with advanced altered capabilities [12].

Existing Review Papers. Before conducting this review paper, we focussed on exploring different related papers to ensure that our work provides a comprehensive overview of the state-of-the-art studies in CPS security. Initially, several informative and knowledge base works were carried out and well represented for securing CPSs. Firstly, [13–17] provides a well-defined survey on SG security and challenges, providing a deep understanding of security issues and solutions in the SG. Secondly, some survey papers have focussed on providing a specific comprehensive overview of SG networks [18–20]. These papers focussed on illustrating different network architectures that can operate ICSs, what available protocols need to be implemented and their limitations. Thirdly, one important aspect is to explore tools available in this field to help monitor SA in these systems. It should be considered that some work mentioned before has discussed the steps of monitoring SA. However, only a few works have conducted tools and techniques for constructing SA. The authors in Refs. [21–23] were focussed on listing tools used in CPSs for many purposes. Yet, these papers lack the exploration of other tools at each step to identify, monitor, alert and assess.

Our Contributions. While all survey papers mentioned above have covered SG aspects such as security, network, tools and threats, several limitations have been identified. One issue is that there is a need for comprehensive work that covers and links these available tools and techniques to utilise them to improve security and robustness for effective SA. Another issue is that while various papers were conducted to evaluate critical assets in the IT field from different perspectives, such as complex communication networks, vulnerabilities, physical security etc. In Refs. [24–29], there is little focus on evaluating OT assets, which can be considered an important issue that needs to be covered to ensure that the field of CPSs is equivalently secured from both OT and IT aspects. Additionally, while conducting this research, it has been found that there are no relevant existing review papers exploring studies for evaluating asset criticality in different CPSs. Therefore, the main contributions of this review paper are as follows.

- The paper provides a comprehensive background of available research and techniques for building a SA platform by exploring asset discovery in ICSs, their available tools, techniques and limitations. The evaluation deeply explores asset identification, ICS communication protocols deployed and vulnerability detection, which can help recognise and utilise the appropriate tools available in this field.
- It evaluates existing techniques that can be used to classify these assets based on their criticality and lists the most important significant cyber threats that can occur in these systems.
- The paper reviews the solutions and simulation environments used for critical assets identification in power system CPS. More specifically, the paper discusses available power systems, network simulation and integrated CPS simulation

tools that are used to create a co-simulation to mount cyberattacks and evaluate the consequences on assets and on the physical system.

2 | SYSTEM AND RELATED TERMINOLOGIES

This section provides a unified base that can be used to illustrate the CPS's infrastructure. Moreover, the section continues to introduce any terminologies that can appear when exploring related work, tools and solutions that have been implemented in such systems.

- **Cyber-Physical Systems** can be defined as the integration between computation and physical processes. CPSs use computer hardware, software and a communication network to control physical processes in manufacturing and other fields [30]. Moreover, based on the National Institute of Standards and Technology Framework for CPSs [31], the SG is considered one of the many implementations of a CPS due to its heterogeneity environment and the need to determine positive emergent behaviours.
- **Situational Awareness** can be described as the perception of the current state and its consequences for the present and the future [32]. In terms of CPS cybersecurity, SA is used to capture and understand the threat information of both IT and OT infrastructures, identify a comprehensive, real-time view of cyber threats on key components and gain knowledge on potential actions an adversary can take to target assets [33]. SA can be vital to propose the best remediation plan to avoid possible cybersecurity consequences that can occur in such systems.
- **Operational Technology** can be characterised as all resources used to monitor any physical process. OT contains ICSs or consists of industrial resources such as factories, machines and networks [34]. Moreover, IT has been integrated with OT to monitor and control physical processes inside CPSs using IT technologies in recent years.
- **Smart Grid** is an electricity network that can be operated in an automated manner by enabling digital technology to efficiently supply electricity to consumers, as illustrated in Figure 1 [35]. Moreover, based on its definition, SG is considered an implementation of a CPS where a combination of OT equipment is integrated with IT infrastructure.
- **Industrial Control Systems** as shown in Figure 2, ICSs are a combination of several control systems that work together to achieve an industrial objective, such as energy distribution and manufacturing [36]. Additionally, these types of control systems can be listed as follows:
 - *Supervisory Control and Data Acquisition (SCADA)* is the main element of the ICS network. Moreover, these systems receive measurement data and monitor and control field equipment in real-time based on predefined control commands [37].
 - *Human-Machine Interface (HMI)* can be considered the main link between the operators and the ICS process.

This component allows the operator to monitor the industrial procedure, change control settings and involves software and hardware components.

- *Programmable Logic Controller (PLC)* falls under the ICS controller category and is used to monitor and control industrial systems. Moreover, this can be done by receiving measurement data from an IED (sensor), executing a logic command if needed and then sending the command to an actuator.
- *Intelligent Electronic Devices (IEDs)* can collect and send different types of data and have the ability to communicate with different components inside the ICS. Sensors/actuators are classified as IEDs in CPSs. Sensors/actuators provide the functionality to receive measurements from lower levels and send them to the controller to validate the progress of events and perform any actions by sending them to the actuators.

3 | ASSET DISCOVERY AND IDENTIFYING CYBERSECURITY ISSUES

Comprehensive information about OT and IT resources and physical access control systems will help identify problems and issues inside CPSs. Additionally, Multi-Intelligent Body Systems (MIBS) can be used in CPSs to enhance their performance and efficiency. In SA, MIBS can offer real-time monitoring and analysis of various data streams, and applying

advanced analytics will allow multiagent systems to identify behaviour and anomalies in the data [38, 39]. The data collected from OT, IT, physical access control, and MIBS can be used to have a comprehensive architecture that provides SA to analyse, capture and store real-time or near real-time data. According to the ICS Information Sharing and Analysis Centre (ICS-ISAC), the four components that can be applied to build SA for ICS are as follows: identify (the objectives, structure and skills of an organisation), inventory (the available hardware/software assets of an organisation), activity (of assets owned by the organisation) and sharing (internal and external communications) [40]. Moreover, all four components described above are categorised into the main three stages of the SA [41] as shown in Figure 3.

The main scope of this study is to provide a comprehensive review of available literature and tools for identifying critical assets, which is considered an important step for constructing a valuable SA. Furthermore, our approach is motivated by studies that covered critical asset identification in cyber-physical SG [42–44], also by including asset interdependencies between different layers inside the SG (e.g., cyber, and physical layers) or between connected CPSs (e.g., SG, and oil and gas) [45–48]. Therefore, this section is divided into four subsections based on the flow chart presented in Figure 4. The first subsection is a comprehensive review of the literature and tools used to identify assets, system components and interdependencies for constructing SA. The second subsection explores the techniques used to assess risks (vulnerabilities, threats and consequences). The third subsection examines different methods to prioritise assets by classifying them based on their criticality. The fourth subsection covers future directions, open issues in this field, and lessons learnt. Lastly, Section 4 discusses the final step illustrated in the flow chart, which utilises simulations to evaluate impacts once a critical asset has been compromised/identified.

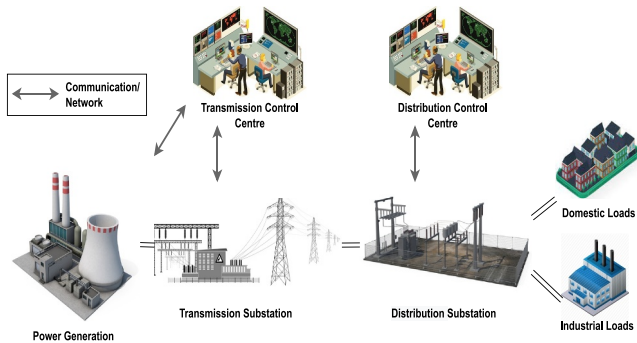


FIGURE 1 Smart Grid (SG) conceptual reference model.

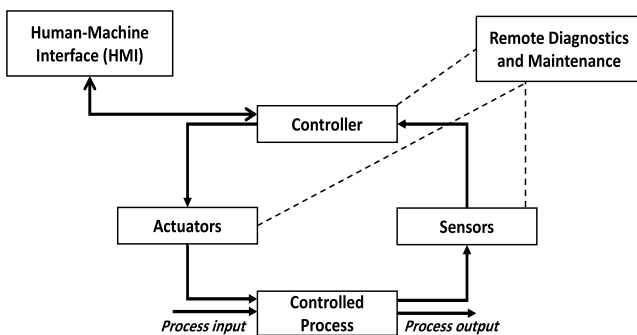


FIGURE 2 A representative system with various Industrial Control System (ICS) components.

3.1 | Identify assets, systems and networks

To gain comprehensive knowledge for developing SA, one essential step that needs to be implemented in any environment is identifying all assets, components and networks that exist in systems. Moreover, asset discovery can help systems

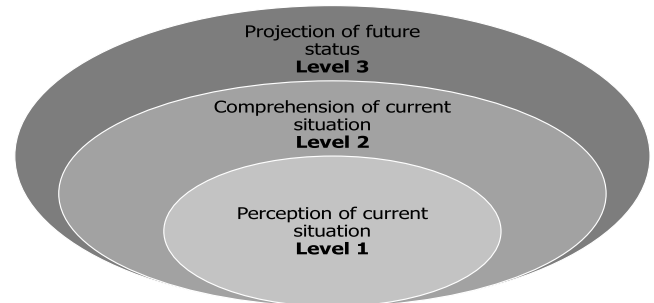


FIGURE 3 Situational Awareness (SA) stages in Industrial Control System (ICS) systems.

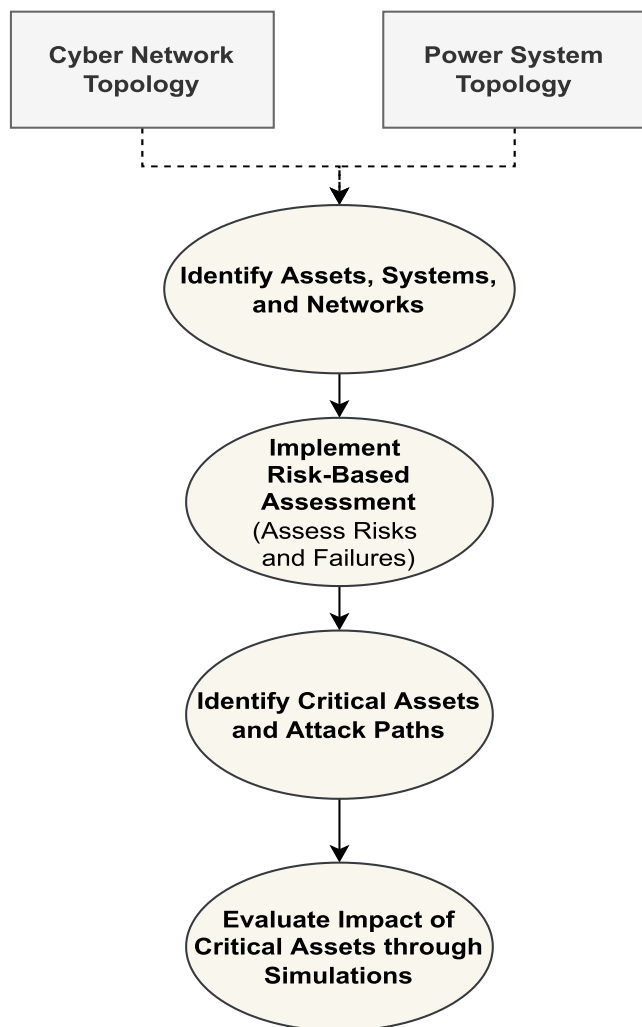


FIGURE 4 Flowchart of implementing asset discovery, assessing risks and failures, and identifying and evaluating critical assets.

ensure a robust recovery process, maintain security configuration and manage patches for many software/hardware [49]. Figure 5 shows an example of asset inventory within an SG environment. However, discovering assets in OT resources inside SG systems is not the same as in IT; these are time-critical. Some are not connected to the network and cannot be discovered with traditional discovery tools [50]. Hence, choosing the appropriate tools available in the market with proper asset discovery techniques that must not affect the process is essential [51]. These systems are time-critical, and failure to operate them is not tolerated; the inability to use them has the potential to result in severe complications, including blackouts, serious injuries to individuals, service interruption and power overloading.

Smart Grid shares common components, such as PLCs, Remote Terminal Units (RTUs), SCADA, and HMIs, which can be found in other CPSs. Table 1 illustrates three techniques used to identify and discover the common assets that can be found in SG and other CPSs. Furthermore, the three techniques can be listed as active, passive and hybrid scanning.






 Hardware	<ul style="list-style-type: none"> • PLC • RTU • IED • Servers
 Software	<ul style="list-style-type: none"> • SCADA • Operating systems • Firmware Development tools
 Staff	<ul style="list-style-type: none"> • Permanent • Sub-contracted
 Information	<ul style="list-style-type: none"> • Databases • Documentation • Manuals
 Network	<ul style="list-style-type: none"> • Routers • Switches • Firewalls

FIGURE 5 Example of asset inventory and classification in Cyber-Physical Systems (CPSs).

Each technique has its characteristics and approach for finding different system assets, and these features sometimes can affect the system's main mission. For instance, the active scanning technique expects full system information from the device as a response, which sometimes distracts the device from performing the main task, causing latency in the overall procedure [60]. Several studies argue that passive scanning is the safest option to discover ICS/OT resources in such an environment [55, 61–63]. These studies argue that passive scanning can only listen without intercepting or asking for a response from assets. However, passive scanning can only bring limited information into account and cannot discover an asset that is not connected directly to the network system [59]. Moreover, passive scanning cannot identify non-IP assets in such an environment [21]. Other studies argue that active scanning can be implemented in CPSs without affecting the system functionality [52, 59]. Additionally, they maintain that it is possible to discover assets actively by using native ICS protocols such as Siemens s7comm (S7 Communication) and Modbus, but this approach is not suitable for handling any sensitive assets [59]. Other providers [64, 65] argue that a third option, a combination of active and passive scanning, can be implemented using passive scanning to gather data from network traffic while sending out active queries as needed. This technique, if applied appropriately, can provide useful information without interrupting any ICS assets from performing their main tasks.

Lastly, choosing an execution technique for asset discovery depends on the organisation's goals and the requirements or information needed to be collected from the system. These discovery techniques can be applied by deploying them into specific tools. One main challenge is the need to differentiate between asset discovery tools applied to OT and IT. Therefore, Table 2 illustrates a broad review of the asset discovery tools used for ICSs and maps them based on available features such as vulnerability detection, any knowledge (e.g., manufacture, system OS, last update, etc.) provided, ICS protocol applied and system visualisation. Furthermore, some listed tools can be integrated easily with other tools, which helps provide comprehensive asset information for organisations. This integration is vital for collecting information to build SA. Additionally, it should be highlighted that some tools mentioned in

TABLE 1 Analysing techniques for asset discovery.

Methods	Description	Advantages	Limitations
Active scanning [52–54]	A technique that uses active network communications to identify devices in the environment.	Identifies assets with more valuable information for ICSs. It can be implanted with stand-alone tools or even commands into the network.	Lock up network interfaces and exhaust CPU resources. It can introduce additional latency into the environment.
Passive scanning [55–57]	Passive scanners transparently intercept and listen to traffic already traversing the network.	Does not actively poll network-connected devices. It can prevent devices from becoming unstable or crashing, leading to a denial of service and posing an immediate safety risk for humans and the environment.	Any device not communicating with the passive discovery sensor will go undiscovered. The usefulness of a deployed passive scanner would be greatly reduced if other communications (e.g., radio connections, modems) were used.
Hybrid scanning [58, 59]	Combines active and passive methods, using active techniques as an enabler for passive techniques.	An example of this would be to use the address resolution protocol (ARP) technique to force all traffic on a network through a central host, allowing the host to be detected and classified by a passive sensor.	It is possible to inherit the same disadvantages that exist in active scanning if implemented wrongly.

Table 2 are marked as a hybrid because these tools can use both active and passive in conjunction or perform both methods independently each time they are deployed.

Based on the steps identified by ICS-ISAC for building SA, this section has discussed the first two segments, identify and inventory. Nevertheless, activity and sharing are yet to be covered for developing a complete SA architecture. These two remaining elements are vital for understanding connections and activities between assets identified in CPSs, which in the cybersecurity context can help recognise that direct and indirect elements are most likely to be compromised and provide the ability to prioritise key components. One approach for demonstrating connectivity between assets is dependency modelling. According to the authors in Ref. [106], dependency can be defined as the correlation between two or more elements in which modifying a component's state can cause changes to other components' conditions. Dependency modelling can be either component-driven or system-driven, depending on the levels of abstraction defined in the chosen risk management technique [107]. Dependencies can be constructed on several relationships that components have, and according to the authors in Refs. [108, 109], some of these can be listed as follows.

- *Cause/Effect Dependency*: This appears when a component is affected by the operability of another component.
- *Location Dependency*: This occurs if components need to be operated within the same or different location.
- *Resource Dependency*: It appears when a component depends on the resource that exists in another component.
- *Input/Output Dependency*: This can arise when a component needs to request/deliver information from another component.

Various works have been presented for dependency modelling in several sectors of CPSs [110–113]. Though this review focussing on defining critical components in SG CPSs,

Table 3 provides studies conducted using component-based dependency modelling based on their connections. Furthermore, the table categorises each work based on the approach implemented, the type of relationships deployed and their limitations.

3.2 | Assess risks and failures

Another step needed to be implemented is to assess risks and failures assigned to all types of assets identified within an organisation. Assessing risks and possible failures is vital for building and moving to the next stage of SA. It enables security analysts, business decision-makers or operators to perceive and comprehend the current situation [121], which will help analysts prioritise their resources based on the achievement of desired goals and objectives. Therefore, this subsection reviews possible techniques for identifying risks and failures in CPSs.

Table 4 illustrates several works that have been done to apply different risk/failure techniques inside the SG system. Moreover, it should be noted that the risk is a result of **likelihood** (*threats exploiting vulnerabilities or potential failures*) multiplied by **consequences** (*the impact specified for an organisation, e.g., business, operations, environment, economic and safety*) [142]. However, one challenge is reducing the uncertainty of a consequence. One solution is that this can be done by including as much information as possible, such as professional judgement, models, expectations, datasets etc. into the risk computation. Another approach to reducing uncertainty was proposed by the authors in Ref. [133], which considered several scenarios (including their description, likelihood and potential impact) that could be used to answer three questions: *What can happen? How likely?* and *What is the impact if the scenario successfully occurred?* The illustrated techniques were evaluated based on their application, background knowledge, scenarios included and the ability to create undiscovered scenarios.

TABLE 2 Tools for Industrial Control System (ICS) asset discovery.

Tools	Technique			Ranking		Full knowledge for assets	Linked with other tools	ICS protocols				System visualisation		Open-source/ Commercial
	Passive	Active	Hybrid	Vulnerability detection	Role	Hierarchy		Modbus	DNP3	S7comm	Ethernet/IP	Profinet	SNMP	
Grassmarlin [66]	✓						✓	✓	✓	✓	✓		✓	Open-source
Splunk [67]	✓			✓			✓						✓	Open-source
Spiceworks [68]	✓						✓						✓	Open-source
OWASP [69]	✓			✓	✓		✓	✓	✓		✓			Open-source
Dragos [70]	✓			✓	✓		✓	✓	✓	✓	✓		✓	Open-source
Tenable.ot [71]			✓	✓	✓	✓		✓			✓			Commercial
Wireshark [72]	✓				✓		✓	✓	✓	✓	✓	✓		Open-source
S7-info [73]		✓			✓					✓				Open-source
SCADA-CIP [74]		✓			✓		✓				✓			Open-source
ETTERCAP [75]	✓			✓			✓				✓	✓		Open-source
Verve [76]	✓			✓	✓						✓			Commercial
CyberLens [77]	✓			✓	✓		✓	✓	✓		✓	✓	✓	Open-source
Snipe-IT [78]			✓					✓		✓	✓			Open-source
Airbus [79]			✓	✓	✓					✓	✓			Commercial
Sophia [80]	✓						✓	✓		✓	✓			Open-source
OT watch [81]	✓			✓	✓			✓	✓	✓	✓			Commercial
Applied risk [82]	✓			✓					✓			✓	✓	Commercial
SCADA-tools [83]		✓								✓		✓		Open-source
ModScan [84]		✓			✓		✓	✓						Commercial
ICS-Hunter [85]		✓			✓					✓	✓			Open-source
Plescan [86]		✓			✓		✓	✓					✓	Open-source
NetworkMiner [87]	✓				✓		✓	✓		✓	✓			Open-source

(Continues)

TABLE 2 (Continued)

Tools	Technique			Ranking		Full knowledge for assets	Linked with other tools	ICS protocols				System visualisation		Open-source/Commercial
	Passive	Active	Hybrid	Vulnerability detection	Role			Modbus	DNP3	S7comm	Ethernet/IP	Profinet	SNMP	
Lansweeper [88]	✓			✓	✓					✓			✓	Commercial
OpenVAS [89]	✓			✓	✓		✓	✓		✓			✓	Open-source
Axonius [90]			✓	✓	✓	✓							✓	Commercial
ModbusScanner [91]	✓				✓		✓	✓						Open-source
BICS [92]	✓			✓	✓						✓			Commercial
PLC-scanner [93]		✓			✓		✓					✓		Open-source
AlienVault [94]	✓			✓		✓							✓	Commercial
SCADA/PLCScanner [95]	✓				✓		✓	✓						Open-source
Modbusdiscover [96]	✓				✓			✓						Open-source
ICSmaster [97]	✓				✓		✓	✓		✓				Open-source
Lengnr [98]			✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	Commercial
Nessus [99]	✓			✓	✓		✓	✓	✓	✓	✓	✓	✓	Open-source
S7scan [100]	✓					✓				✓				Open-source
Redpoint [101]			✓				✓	✓		✓				Open-source
CyberX [102]			✓	✓	✓			✓	✓	✓	✓		✓	Commercial
Nmap [103]	✓				✓	✓	✓	✓	✓	✓	✓			Open-source
Nmap-SCADA [104]	✓				✓		✓			✓				Open-source
TripWire [65]			✓		✓	✓		✓	✓		✓		✓	Commercial
DOT by Awen [105]			✓	✓	✓	✓		✓	✓	✓	✓		✓	Commercial

TABLE 3 List of studies conducted using dependency modelling for critical assets identification in the Smart Grid (SG).

Work	Contribution	Type of relation			Approach			Limitations
		Cause/Effect dependency	Location dependency	Resource dependency	Input/Output dependency	Graph based	Matrix based	
[114]	The work proposes an approach for modelling the intra- and inter-dependency of a micro-distribution network. Additionally, four parameters were proposed: the impact of dependency, the susceptibility of dependency, the weight of dependency and the criticality of dependency for quantitative assessment of the characteristics of dependencies.	✓				✓		This work considers buses only as electrical nodes in addition to routers and multiplexers as information and communications technology (ICT) nodes.
[115]	This work presents a security model that can show the privilege states in a large architecture and evaluates possible paths that attackers could exploit. Moreover, the quantitative information produced from the model is used to identify information dependencies to enhance the risk management processes.			✓		✓		The proposed work focusses on privileged states. There is little focus on identifying critical nodes, and the main goal is identifying information dependencies only.
[116]	The work investigates the cause-and-effect dependency between the SG and ICT components by categorising and defining the state of the SG assets and their impact once an ICT component fails.	✓				✓		The main aim of this work is to show the dependencies between ICT and power components if ICT nodes fail. There is little effort in modelling power components, and no information was introduced regarding compromised nodes from cyberattacks.
[117]	This work provides an overview of different techniques for modelling dependencies between various critical infrastructure systems. Moreover, it delves into the interdependency approaches at transmission and distribution levels to outline the validity of using these dependency approaches on real-time systems.	✓					✓	This work covers interdependence between critical infrastructure and shows interdependencies at transmission and distribution levels. Yet, this work is focussed on covering electric nodes only, and there is little focus on cyber nodes.
[118]	The work proposes a framework to assess the impact of cyberattacks on SG. Furthermore, this study presents a cause-effect relationship between cyber and physical components.	✓				✓		This work focusses on showing the physics of the interaction for power nodes and uses the functionality for cyber grid elements. However, in terms of cybersecurity assessments, the evaluation was conducted using unauthorised access only.
[119]	This study proposes a wide area measurement system (WAMS) model in an SG combined with graph-based dependency to show the dependency between communication and measurement layers to enhance the SG WAMS resilience.		✓			✓		This work discusses developing a dependency model for SG. However, its main focus is on WAMS. The presented metrics were related to the measuring and communication of WAMS layers. There is little focus on other cyber assets, and the evaluation was only conducted on PMUs and optical ground wires.

(Continues)

Work Contribution

Work Contribution	Type of relation			Approach		Limitations
	Cause/Effect dependency	Location dependency	Resource dependency	Input/Output dependency	Graph based	
[120] The work proposes a dependency graph using phasor angles to model SG fault detection. Additionally, phasor angles were driven as random variables in Gaussian Markov random field (GMRF) to determine fault detection and the localisation of transmission lines.				✓	✓	The work has been conducted to address fault diagnosis in power grids using the conditional correlation matrix of the GMRF. Yet, it lacks identifying cyber nodes, cybersecurity challenges were not included and the evaluation was applied to limited hierarchical power systems nodes

Table 5 illustrates a brief description of common risk assessment and asset identification methodologies. The table

The next phase that needs to be studied is to monitor CPS's SA regarding asset criticality. Distinguishing key assets in CPSs is vital and will help the organisation develop the best remediation plan in advance to avoid catastrophic consequences. Moreover, it should be considered that implementing this step is a challenge due to the different characteristics of each CPS. For example, one of the different assets inside an SG is a transformer that converts the voltage into either step-up or step-down, and the failure to protect such an asset is not tolerated; currently, there is no universal method to identify these assets. Therefore, this section discusses identifying critical asset methodologies, listing key requirements and exploring techniques and related work conducted in this field. Initially, based on Ref. [143], two requirements must be met for successful asset identification in critical infrastructure. The first requirement is *qualitative*, which refers to meeting certain soft criteria to develop an efficient identification methodology. Moreover, The National Infrastructure Protection Plan [144] listed these criteria as completeness, reproducibility, documentation and defensibility, which can be used to evaluate the critical identification methodology of CPSs. The second requirement is *quantitative* which can be defined as solid measurement criteria for the critical asset identification process. These measures are referred to as the assets weight score, the organisation's mission criteria and scoring guide and the asset identification process, which was covered in 3.1. Therefore, according to the authors in Refs. [143, 144], Figure 6 shows a complete map of achieving the following requirements for critical asset identification.

- **Completeness:** This represents the requirement where an approach provides comprehensive component evaluation (threats, vulnerabilities and consequences) into the many different critical infrastructures.
- **Reproducibility:** The risk methodology should ensure that the proposed results are qualified and comparable with different sectors, making it easy to evaluate risks against other CPSs.
- **Documentation:** The methodology must document the approach, techniques and information conducted, any remediation plans applied or suggested and the users involved.
- **Defensibility:** The proposed risk methodology should be error-free, reducing uncertainty and efficiently integrating its components.
- **Elements:** Requirements, such as asset identification list, criteria, weighted score to indicate asset criticality, scoring guide and how it is applied, are used as input to the risk methodology.
- **Components:** These include the scope of the methodology (systematic or unsystematic), the applied approach used (network, function or logic based) and how the information gathered is evaluated.

Table 5 illustrates a brief description of common risk assessment and asset identification methodologies. The table

TABLE 4 Summary of risk/failure techniques used in Cyber-Physical System (CPS).

Technique	Description
Fault tree analysis (FTA) [122, 123]	<ul style="list-style-type: none"> • It focusses on a system's safety and reliability. • It can be used for observing the impact and likelihood of equipment failure. • It allows experts to be involved in obtaining much background knowledge about the system. • It can reflect the logical relationships and interdependencies between components. • It can show complete information about a malicious attack using FTA when used in a cyber threat context. • Complete information/components about the system are needed. • The core function of this analysis is to predict equipment failure. • As it depends on the probability of failure, it can be integrated with PRA
Event tree analysis (ETA) [124, 125]	<ul style="list-style-type: none"> • It is a qualitative system analysis similar to FTA. • The key difference is that it considers impacts using inductive reasoning. • It assumes that each event being analysed has two results (success or failure). • As it depends on the probability of failure, it can be integrated with PRA.
Bow-Tie analysis [126]	<ul style="list-style-type: none"> • It is an analysis that is a combination of FTA and ETA. • It uses ETA to reflect the consequences of an incident, while FTA is used to learn what may have caused the incident. • It can create several unconsidered scenarios that will comprehensively help to understand a system failure.
Attack tree [127, 128]	<ul style="list-style-type: none"> • A threat model technique describes how an attacker can attack a target through the network. • Unlike event and fault trees, the main focus of the attack tree is on malicious activities, not failure activities. • ETA and FTA can be linked to attack trees for a comprehensive malicious and failure analysis.
Monte Carlo simulations [129, 130]	<ul style="list-style-type: none"> • A random analysis establishes unconsidered points and scenarios that can determine a system's availability and operability. • As this simulation created random initial values, it requires a long-running time to obtain valid results and deep data. • This technique aims not for a cyber threat context, but it generates random situations that have not been considered before and can include cyber threats.
Failure modes, effects and criticality analysis [131]	<ul style="list-style-type: none"> • It is a hazard analysis based on skills, engineering best practices and standards. • It can integrate standards and good practice policies and analyse the different approaches for node failure along with its impact. • As it focusses on specific components, it can also be used to analyse components' criticality. • This analysis focusses on the impact but not on the reasons for the impact, but using FTA at the same time can help with this.
Hazard and operability (HAZOP) method [132]	<ul style="list-style-type: none"> • The main usage is for hazard analysis, and it is the most applied in CPSs for this kind of analysis. • It divides the system into components and will provide a strict assessment of the impact on each one. • It can be used for cyberattack analysis when assuming each component/process is affected by a cyber threat.
Probabilistic risk assessment (PRA) [133, 134]	<ul style="list-style-type: none"> • It is a scenario-based approach that utilises three questions as follows: <ol style="list-style-type: none"> 1. What can go wrong? 2. How likely? 3. What is the impact? • Its main usage is for accident analysis, and it is not designed for cyberattack analysis.
Markov models [135]	<ul style="list-style-type: none"> • A risk analysis based on Markov models. • It is similar to Monte Carlo simulations and can be used with BN for comprehensive failure and malicious scenarios.
CARVER and MSHARPP [136]	<ul style="list-style-type: none"> • CARVER (criticality, accessibility, recuperability, vulnerability, effect and recognisability) and MSHARPP (mission, symbolism, history, accessibility, recognisability, population and proximity) are assessments that analyse the weaknesses of a system from an attacker's perspective. • Using CARVER helps to determine the criticality and vulnerability of components in the system, resulting in a list that has critical asset information.
Game theory [137–139]	<ul style="list-style-type: none"> • Game theory in cybersecurity is modelling and analysing the behaviour of attackers and defenders in different scenarios. Game theory helps to recognise the strategies and motives of attackers and develop effective defensive measures. • Game theory is used to analyse the situation of two or more participants depending on how the context is listed. • The outcome is a useful resource to minimise risk for an organisation and, in contrast, raise the danger for an adversary.
Bayesian network (BN) [140, 141]	<ul style="list-style-type: none"> • A conditional probabilistic method based on theory depends on a piece of evidence to validate whether a specific scenario is possibly true, fully true or false. • Unlike PRA, this technique can consider the context of cyber threats. • The main difficulty of BN is that it needs evidence to calculate its belief but obtaining real-time evidence in a CPS is quite difficult.

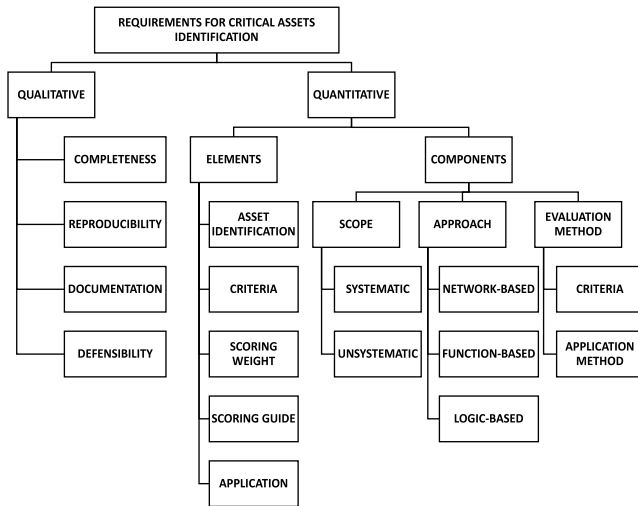


FIGURE 6 Requirements for critical assets identification.

also maps the listed methodologies to the abovementioned requirements in Figure 6. Nevertheless, aiming to secure and identify critical assets in power systems, The North American Electric Reliability Corporation Critical Infrastructure Protection proposed a set of standards applied specifically to cybersecurity. The main aim of these standards is to legalise, implement, monitor and control the security of power systems [145, 146]. NERC CIP consists of nine rules, and one significant rule is critical cyber asset identification *CIP-002*. Moreover, this standard requires identifying critical assets through implementing risk assessment methodologies, and assets will be declared critical if any compromise may threaten electric reliability [147].

Table 6 illustrates a survey of several works that researchers have conducted to prioritise and classify assets based on their criticality in the SG. The studies analyse and justify their work from different perspectives, such as business, impact and equipment health. In addition, they continue to validate their proposed methods by conducting different scenarios, such as natural fails, operator miss behaviour and, most importantly, cyberattacks.

3.4 | Lessons learnt

Determining the best technique for asset discovery in CPSs is not straightforward. Asset discovery depends on the characteristics that the organisation defines. For instance, IT asset identification can be used with passive and active techniques, but system availability and latency should be considered when dealing with OT assets. Recently, new techniques have surfaced that use ICS protocols to deal with OT, which can be considered promising. As mentioned in section 3.3, some critical asset identification requirements are criteria and asset weight scores, which should be chosen based on their distinctive characteristics. Consequences and impact on CPSs are focussed in a specified system area, for example, SCADA,

PLCs, and HMI, but there is little focus on the lower levels (physical process), that should be explored in great details. Risk techniques have different aims and goals, yet they should be chosen to meet two main goals: (1) obtaining as much threat knowledge as possible and (2) including more scenarios that are not discovered yet, which can enhance the SA process in these systems.

4 | MODELLING, SIMULATION AND EVALUATION

Information aggregated from CPSs, such as system components, assets criteria, interdependencies and critical identification, needs to be validated in order to evaluate the situation in different scenarios. Moreover, in the case of the SG, it is impossible to validate proposed approaches for risk assessment in real-life systems [169]. However, the possible way to do that is by applying them to SG simulations that simulate power from generation to distribution, similar to a real case of SG. Likewise, an appropriate simulator should consider three aspects: power, cyber and transmission. Table 7 lists the existing simulation tools that can be used to cover the power system, cyber security and communication network aspects in the SG. These aspects in one simulator can help present the SG systems and their communication, physical devices, protocols and control centre systems. Smart Grid simulations can help to explore complex attacks similar to the real world, for example, the Ukraine power grid cyberattack [4], which helps recognise the impacts and assess components that are most likely to be targeted and affected in such a critical system. Therefore, this section lists tools used to simulate power systems, communication networks, control centre systems and related work conducted to apply attack scenarios and failure analysis into SG simulations that aim to validate asset criticality.

4.1 | Electric power simulators

This subsection illustrates different tools available for power simulators that are used for power generation, transmission and distribution, similar to the real-life power grid.

- **PowerWorld:** A commercial tool used for power system simulators provides a comprehensive simulation for generation, transmission and distribution. Furthermore, PowerWorld gives the user different options, for example, choosing fuel types for generators and specifying maximum and minimum power transmitted, which can be used to mimic real-life scenarios for SG. PowerWorld can be integrated with other tools using SimAuto, making the case accessible through MATLAB, Python and Visual Basic [170–172].
- **PSS:** A commercial power system simulator (PSS) tool was developed by Siemens that includes different solutions to

TABLE 5 Comparison among methodologies for critical asset identification.

Methodology	Description	Scope		Approach	
		Systematic	Unsystematic	Network-based	Function-based
NCIPP [148]	It is used by the department of homeland security for critical infrastructure security and resilience by assessing and analysing critical infrastructure threats, vulnerabilities and consequences.	✓		✓	✓
EPCIP [149]	The European programme for critical infrastructure protection (EPCIP) is an optional methodology that enables information-sharing among the European Union (EU) member states and other critical infrastructure protection (CIP) group participants.	✓		✓	
DCIP [150]	The US department of defence employs the CIP framework to identify, rank and protect critical infrastructure and its areas from terrorist attacks.	✓			✓

TABLE 6 List of solutions for identification of critical assets.

Work	Contribution	OT network					Limitations
		Process level (L0)	Basic control (L1)	Supervisory control (L2)	Site operation (L3)	Enterprise network (L4/5)	
[151]	The paper discusses the development of three criticality metrics by modelling an attacker's opportunity to compromise several hosts. The work also presents a system design to validate each metric in real-case scenarios.	✓	✓	✓	✓	✓	Three novel metrics were presented, yet the focus was only from an attacker's opportunity perspective with no focus on the lower levels.
[152]	The work proposes critical asset classification in industry 4.0; primarily, the classification is based on the business impact while a cyberattack compromises the system. Additionally, the paper introduces a correlation between critical assets and the business impact for improved decision-making in cybersecurity policies.					✓	This work implemented several metrics to evaluate critical assets, but it mainly focussed on potential business impacts.

(Continues)

TABLE 6 (Continued)

Work Contribution	OT network					Maintenance/ Business Health		Limitations
	Process level (L0)	Basic control (L1)	Supervisory control (L2)	Site operation (L3)	Enterprise network (L4/5)			
[153] This paper proposes a critical analysis approach to identify key power lines in power systems for maintenance improvement. Moreover, the work continues to offer automation for the proposed analysis by utilising existing IT solutions in this field.						✓		The context of ICS systems was not identified in this work, and the evaluation was conducted on limited nodes for implementation only.
[154] The work offers a long-term health index prediction for power assets using a sequence learning-based method. Furthermore, the method was assessed using actual utility data for validation and asset health prediction.	✓					✓		The main limitation of this work was that it focussed on the health index in energy management systems.
[155] The work illustrates different approaches that can be used to identify critical information assets and communication network components. In addition, the paper delves into cascading effects while targeting communication network assets in critical infrastructure.		✓						There was no application of this method nor a specific focus on a specific zone.
[156] This study proposes an ICS security assessment framework based on open-source intelligence. Moreover, the work consists of three stages: Data collection, assessment and ranking critical components using qualitative and quantitative metrics.		✓	✓	✓	✓			This work aimed to build an ICS ranking tool, but it was too general in CPS, making it hard to be applied to the process level since different CPS systems have different factors.
[157] This work offers a multiple attribute decision-making (MADM-based) ranking algorithm that can be used for critical asset identification and ranking. Moreover, another contribution is the multiple vulnerability node rank, which uses vulnerability information for cybersecurity classification.		✓	✓	✓	✓			There was little focus on the physical/process level.
[158] The work offers an analytics approach for modelling asset health and network reliability by predicting the remaining life cycle and the ageing of assets. The information used for this approach is obtained from different sources, such as SCADA, geographic information systems and outage management systems.	✓					✓		This work covered lower levels of SG, yet the main focus of the classification was based on predicting the ageing of assets.

TABLE 6 (Continued)

Work Contribution	OT network					Maintenance/ Health	Limitations
	Process level (L0)	Basic control (L1)	Supervisory control (L2)	Site operation (L3)	Enterprise network (L4/5)		
	Business	Health					
[159] The paper utilises asset knowledge, such as performance, location and functionality, to predict the trend of the impact of cybersecurity incidents. In addition, the paper examines both component and system levels to determine the propagation of an impact when the system is compromised.	✓					✓	The evaluation of the proposed method was conducted on a chemical control system, and the impact is quantified based on location and business only.
[160] The work provides an implementation of a proposed approach for asset management in electrical systems. The case was applied to determine critical power transformers within three stages: a) Modelling and estimating temperatures in transformers in the short term, b) estimating the health condition for the medium term and c) estimating the remaining life of the power transformers.						✓	The focus of the proposed framework was mainly on asset maintenance performance and contingencies analysis. There was no consecration of cyber threats or risk assessment.
[161] This work proposes a framework based on the OCTAVE allegro method to rank critical information assets. The framework utilises several decision-support methods, such as simple additive weighting and the analytic hierarchy process, to prioritise risks targeting information assets.					✓	✓	This work aimed to classify critical information assets, and there was no focus on physical devices or lower levels of CPSs. There was no evaluation of the proposed method.
[162] The work implements the cyber attack impact assessment technique to evaluate the impact of different cyber threats. Additionally, the paper provides numerical results for the implemented approach obtained using a chemical process simulation.	✓	✓	✓	✓			The main aim was specified on the closed-loop process control system. In addition, the evaluation was performed on the chemical process model.
[163] This paper provides a solution for identifying key cyber terrains assets. Moreover, the proposed approach explores the dependency degrees among tasks and assets by building a connection between the operational network and the asset vulnerabilities.					✓		This work's main aim was only on cyber assets, and there was no information about network security. Also, the work lacked the identification of physical layer assets or an analysis of their impact.
[164] The work provides an intuitive approach to identifying critical digital assets (CDAs) inside the nuclear reactor domain. Furthermore, the approach was conducted using three different implementations: 1) identifying CDAs with an attack graph tool, 2) identifying CDAs with a purpose-built programme and 3) identifying CDAs with a modified attack graph.			✓	✓	✓		This work focussed on the automatic identification of critical assets. Still, one limitation was a need for manual evaluation, and physical layer assets were not covered. Another limitation of the proposed method was that it could not discover assets in unconnected or isolated networks.

(Continues)

TABLE 6 (Continued)

Work Contribution	OT network					Maintenance/ Health	Limitations
	Process level (L0)	Basic control (L1)	Supervisory control (L2)	Site operation (L3)	Enterprise network (L4/5)		
[165] This paper focusses on the measurement of the sensitivity levels of enterprise assets using enterprise information security management. Moreover, the measurement process is divided into two stages. Firstly, for data assets, the measurement is based on the sensitivity of the data. Secondly, for non-data assets, the measurement is based on their usage patterns and the attributes of users.					✓		The main aim of this work was focussed on the data sensitivity an asset holds, and the data classification applied was on IT assets only. There was no implementation of CPS or other asset criteria.
[166] The work investigates grid-forming inverters by integrating high levels of renewable energy and distributed energy resources in the power system. This integration can reduce the physical and electrical distance between generation and loads in power systems.	✓						The asset criticality focussed on the physical layer and the interactions between inverter base sources and the bulk-power system. However, it lacked other OT layers, and there was no information about cybersecurity threats.
[167] This paper proposes an enhanced cybersecurity risk management (CSRM) for asset criticality, threat prediction and evaluating existing controls. In addition, the paper utilises different approaches for the developed CSRM, including fuzzy set theory for asset classification, machine learning for risk prediction and the comprehensive assessment model for evaluating existing controls.		✓	✓	✓	✓		This work was conducted on a limited range of assets, and there was less focus on physical layer assets. Key performance indicators were defined but on a general basis (availability, confidentiality, integrity, accountability and conformance).
[168] The work aims to present a novel asset-focussed risk management approach for critical infrastructure, with a main focus on asset interdependence and cascading effects. Moreover, implementation is conducted on a running example from an SG system to test the approach validation.				✓	✓		There was less focus on physical layer assets. Asset criteria were defined on a broad scale. The implementation was on limited assets, with no damage analysis.

TABLE 7 Summary of existing simulation tools.

Power system simulators	
PowerWorld	Commercial
PSS	Commercial
MATPOWER	Open-source
DigSilent-Powerfactory	Commercial
PSCAD/EMTDC	Commercial
GridLAB-D	Open-source
Power system simulation toolbox (PSST)	Open-source
OpenDSS	Open-source
PandaPower	Open-source
Homer	Commercial
ETAP PSMS	Commercial
EuroStag SmartFlow	Commercial
EMTP-RV	Commercial
Modelica	Open-source
ObjectStab	Open-source
Positive sequence load flow (PSLF)	Commercial
Hardware – in – the – Loop (HIL)	
Real-time digital simulator (RTDS)	Commercial
OPAL-RT	Commercial
Network simulators	
NS-3 and NS-2	Open-source
OMNeT++	Open-source
NeSSi	Open-source
QualNet	Commercial
OPNET modeller	Commercial
CPS simulators	
ScadaBR	Open-source
OpenSCADA	Open-source
SCADASim	Open-source
OpenPLC	Open-source

Abbreviation: PSS, power system simulator.

integrate them with the simulator. One solution is the PSS SINCAL, which allows communications to be established to achieve transmission and distribution to the grid [173–175].

- **MATPOWER:** This is an open-source tool for power simulation developed using MATLAB language. The tool gives the user the ability to resolve and analyse steady-state power systems and optimisation problems such as Power Flow (PF), Continuation Power Flow, extensible Optimal Power Flow (OPF) and Unit Commitment (UC) along with stochastic, secure multi-interval OPF/UC. Additionally, this tool can be integrated with other tools using PYPOWER [176–178].

- **DigSilent-Powerfactory:** A commercial power simulator tool is used for power, generation distribution and transmission. Moreover, similar to PSS and PowerWorld, DigSilent provides a comprehensive simulation for the SG and can be integrated with other tools, such as MATLAB; however, hardware needs to be deployed within the simulations [179–181].
- **PSCAD/EMTDC:** It is a commercial tool used for power system simulators that simulates power from generation to distribution, giving the user the ability to analyse a power system comprehensively. Moreover, this tool can be integrated with other tools, such as MATLAB, for research/experiment purposes [182–184].
- **Power System Simulation Toolbox:** An open-source tool developed by [185] written in Python code is used for Agent-Based Modelling of Electricity Systems.
- **OpenDSS:** Open Distribution System Simulator is an open-source tool used for power system simulation and can be integrated with other tools due to the availability of the communication (i.e., COM) interface [186].
- **ETAP PSMS:** Power System Monitoring & Simulation (PSMS) is a commercial tool developed by ETAP that provides a comprehensive simulation for the power grid similar to PowerWorld, PSS and DigSilent-Powerfactory. Additionally, there are a few resources on whether or not this simulator can be integrated with other tools [187].
- **Homer:** A commercial tool uses simulation power generation only; this simulator is focussed on simulating energy generation resources, for example, wind, solar power and others. Unlike other tools, Homer cannot be used for other power systems domains like distribution and transmission [188].
- **PandaPower:** This is a Python-based tool that is used for power system analysis by providing PF, OPF, state estimation, topological graph searches and short-circuit calculations. PandaPower is an open-source tool [189].

In addition, other power simulators, Modelica [190], ObjectStab [191], EuroStag SmartFlow [192], EMTP-RV [193] and positive Sequence Load Flow (PSLF) [194], are available and are widely used by researchers to indicate power reliability and security. MATLAB/Simulink can be used to create SG simulations, but one disadvantage is that MATLAB/Simulink cannot produce realistic measurements as well as other reliable power simulators.

4.2 | Hardware-in-the-Loop

Solutions that involve hardware such as OPAL-RT [195–197] and Real-time digital Simulator [198] provide a realistic and real-time simulation environment for power systems. Hardware-in-the-Loop brings many advantages, such as creating a real-time virtual environment similar to real CPSs, which allows the user to test large-scale power systems in real-time. The main disadvantage of this solution is that researchers consider it to be expensive.

4.3 | Telecommunication networks simulators

Simulators can be used along with power simulators to achieve transmission and distribution communication. Integrating network simulators brings several advantages, such as testing complex scenarios for CPSs and implementing specific ICS protocols, for example, DNP3, Modbus/IP, which can help demonstrate cyberattacks through the network. Available tools are NS-3 and NS-2 [199–201], OMNeT++ [181, 182, 202], NeSSi [203, 204], QualNet [205–207] and OPNET Modeller [208–210].

4.4 | Cyber-Physical System simulators

Supervisory Control and Data Acquisition/PLC simulators are used to show measurements/control processes in CPSs. These simulators can receive measurements from sensors deployed in the physical layer of CPSs and perform some logic control conditions already defined inside them to control the physical process by actuators. This operation can help achieve automation similar to real case systems. Some available tools are SCADABR [211], OpenSCADA [212], SCADASim [213] and OpenPLC [214].

4.5 | Co-simulation

It is not easy to create a comprehensive simulation for a specific system. Designing a comprehensive simulation can consume time and money, especially for researchers aiming to analyse a power system for a specific need. One way to avoid that is to combine different available simulations from different levels to establish a power system with telecommunication capabilities for a comprehensive analysis. Co-simulations bring several advantages, allowing researchers to propose novel ideas and solutions that help increase the reliability of energy systems [215]. Additionally, many researchers have proposed their co-simulation frameworks for different domains. Table 8 provides a survey of available co-simulations, briefly describing each work, the power system and telecommunication simulator used in the study and whether it is cybersecurity-focussed.

4.6 | Lessons learnt

The best approach to validate asset criticality, possible threats and equipment failure is to implement them into an integrated simulation. There is little focus on end-to-end comprehensive cyber-physical simulations for analysing impacts and identifying assets. A stand-alone simulator, such as a telecommunication networks simulator to present CPS's cyber layer, is inadequate to assess threats and build SA. In order to validate the consequences of possible threats and build SA for SG CPSs, a proper simulator that covers cyber, physical and transmission layers should be chosen. Cyberattacks, failures

and time delays are possibly found in the cyber layer components, for example, SCADA, IEDs, PLCs and RTUs. Yet, measuring damage and identifying cascading effects can be found in lower layers (physical layers). Linking cyber and physical layers is done by the transmission layer (connection medium), which sends commands to control physical assets via ICS controllers (actuators) and feeds measurements to ICS components using sensors. Moreover, it is important to distinguish between cyber threats that can lead to failures and failures caused by natural events by gathering as much knowledge about these scenarios as possible using risk/failure techniques conducted in CPSs.

5 | FUTURE DIRECTIONS AND OPEN ISSUES

This section lists key open problems while reviewing related studies in this field. Equally, it is important to address them rapidly, as this field is considered globally critical.

5.1 | Scalable data collection

It is one of the biggest issues inside these systems. This can be because (1) availability is an important aspect that should not be affected whatsoever while the system is running, (2) pure OT and legacy system components are installed and serving their purpose without deploying any cyber solutions that can be helpful to avoid increasing cyber threats and (3) the heterogeneity in the environment that exists between industrial protocol and IT protocols makes communication difficult. Moreover, scalable data collection can be divided into three main categories, each of which has many reasons why collecting data from these time-critical systems is difficult. The first is the lack of an overall asset visibility technique that can be used to identify resources without affecting the process continuity. As discussed in section three, each discovery technique available has its characteristics and needs to be applied to the system to collect as much information as needed to build appropriate asset management, which will help reduce and mitigate cyber threats. Second, some industrial protocols communicate in plain text, meaning that any responses received and stored are readable. Furthermore, applying encryption algorithms in these protocols is difficult and can consume time and memory resources, which are limited in industrial components. Therefore, there is a need to have secure communication links, and the storage of the collected data should prevent unauthorised access by applying the appropriate authentication mechanisms.

5.2 | Adapting new techniques

The need for new techniques (such as machine learning) for specific risk type prediction can help different industries rank threats and prioritise assets based on cruelty, risk level and

TABLE 8 List of existing co-simulations for Smart Grid (SG).

Co-simulation	Power simulators													Network simulators						Cyber security domain		
	MATLAB/ Simulink			MATPOWER	PYPOWER	Modelica	GridLAB-D	OpenDSS	DigSILENT PowerFactory		PSCAD/ EMTDC	PSLF	InterPSS	Hardware-in- the-loop	NS-2	NS-3 and OMNeT++	NetSi	OPNET	QualNet	Other		
	PowerWorld																					
EPOCHS [216]										✓					✓							
GECO [217]												✓			✓							
SCADA-Sim [218]		✓														✓				✓		
Lévesque et al. [219]																✓						
PowerNet [220]						✓									✓							
ASTORIA [221]							✓								✓					✓		
CPSA [222]	✓														✓				✓	✓		
Sudnan et al. [223]							✓								✓							
SG-sim [224]								✓								✓				✓		
GridSpice [225]				✓			✓															
Pan et al. [226]		✓													✓							
Souza et al. [227]								✓							✓					✓		
Ni et al. [228]		✓																	✓			
Amarasekara et al. [229]		✓																				
GridAttackSim [230]															✓					✓		
FNCS [231]															✓							
Al-Hammouri [232]																						
TASSCS [233]	✓																		✓	✓		
HELICS [234]															✓							
INSPIRE [235]										✓								✓				
Sun et al. [236]									✓									✓				
ERGrid [237]										✓												
Chinnow et al. [238]																			✓	✓		

calculation. Moreover, threats in CPSs are becoming more advanced with new techniques and resources that can expose many vulnerabilities in OT components. Additionally, risk and threat levels are continuously changing. They can be considered important because predicting and ranking threats can help businesses make appropriate and informed decisions since each business's aim and field can differ from each other. Therefore, applying advanced techniques for detecting threat patterns and accurately measuring risk type and level is needed to improve CPS security using several input types, such as skills, motive, location, techniques, assets resources etc. Using the collected information in machine learning classifiers provides a prediction of risk, which will help organisations apply security mitigation in advance and improve their incident response.

5.3 | Heterogeneity between operational technology and information technology

Another open issue is the heterogeneity between OT and IT from different aspects. Communication between their components to aggregate information is needed; however, enabling such communication and translation can bring vulnerabilities and breaches. As mentioned, industrial control protocols were designed to execute field procedures without considering security aspects. Recently, new industrial protocols were deployed with security features but are mostly incompatible with legacy devices. In addition, physical devices and their operating systems can be vulnerable to cybersecurity threats since most physical devices are outdated or have limited computational capacity and insufficient memory, making it difficult to apply security measurements. Furthermore, specific security solutions need to be implemented here. It is difficult to apply traditional security solutions, such as Intrusion Detection System and encryption methods, to these systems due to the specific requirement for its components and the new sophisticated attacks that have occurred in recent years. Therefore, combining security mechanisms with CPSs must be used, while also considering the requirements for IT/OT components and enhancing the overall security technology in this field.

5.4 | Lack of focus on cascading effects

Cascading effects of cybersecurity risk on interconnected components is another issue that has been raised in CPSs. Moreover, cascading effects can be considered one of the most complicated issues in CPS safety. This issue can be caused by many factors, including natural disasters and physical, technical or human errors, which can initiate a sequence of serious events affecting a system, an entire city or something much bigger. Understanding and exploring interdependencies between systems and analysing (in case a cyber threat is successful) the cascading effects on a targeted asset can help prepare an organisation to make firm decisions to avoid massive disasters.

5.5 | Evaluating and identifying critical assets

Finally, evaluating and classifying assets is an issue that must be addressed in the CPS, either by the damage that can be caused, the cost or even by its capability to achieve a business goal. Assets are not only related to IT components in the enterprise network. Assets are more than that in CPS; they can be hardware/software components run at the operational level (SCADA, PLC, RTU, IED, etc.), human (operators, maintainers, engineers) and data collected from the system, which can be significant for analysis, network communication and physical assets (as in the case of SG generators, transformers, transmission lines etc.). Furthermore, the need to evaluate and focus on physical assets in criticality when cyber threats arise is important nowadays, and a specific framework should exist since each industry runs different physical devices. Physical devices in the SG are not the same in water treatment, oil and gas or nuclear systems. Criticality evaluation can be used regarding the type of connection, operator management, lifespan and health and potential physical damage. Having comprehensive information from the asset visibility can help build specifically designed and appropriate asset management, which enhances the SA for these systems. Combining all this aggregated information will allow them to be used in advanced alerting capabilities, addressing the need to construct an alerting system that combines possible cyber threats into such a system as well as failure analysis for all types of equipment and devices.

6 | CONCLUSION

In this study, stages of monitoring SA of SG have been surveyed in terms of the following facets. At the beginning, we discussed the different approaches that can be used to identify IT and OT assets, listing their limitations and the tools applied in this field. Then, we provided a detailed analysis of the studies, frameworks, methodologies and risk techniques that can be used for critical asset identification and evaluation in power systems. Afterwards, we presented an outline of the methods used to evaluate the consequences on the cyber and physical system to emphasise the effects of failing to secure SG assets. Furthermore, the open issues and future directions for monitoring SA and critical asset identification are carefully summarised at the end of this study.

As it is reviewed, we have noticed that security solutions, along with critical asset identification, were mainly focussed on IT assets, and currently, there is little focus on looking at physical OT assets. Gathering complete information about OT assets is essential for monitoring power systems SA. Nevertheless, any discovery techniques/tools implemented need to be chosen in a way that does not affect the system's functionality, as OT assets are considered time-critical and cannot afford to disturb their main tasks. Moreover, integrating sophisticated techniques such as machine learning can help predict specific risk types and keep up with the continuous change of existing cyberattacks.

AUTHOR CONTRIBUTIONS

Yazeed Alrowaili: Conceptualisation; Formal analysis; Methodology; Writing – original draft; Writing – review & editing. **Neetesh Saxena:** Conceptualisation; Formal analysis; Methodology; Supervision; Writing – original draft; Writing – review & editing. **Anurag Srivastava:** Conceptualisation; Methodology; Writing – review & editing. **Mauro Conti:** Methodology; Writing – review & editing. **Pete Burnap:** Conceptualisation; Methodology.

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no conflict of interest.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

ORCID

Yazeed Alrowaili  <https://orcid.org/0000-0002-3710-2612>

Neetesh Saxena  <https://orcid.org/0000-0002-6437-0807>

REFERENCES

- Knight, J.C.: Safety critical systems: challenges and directions. In: Proceedings of the 24th International Conference on Software Engineering, pp. 547–550 (2002)
- Johnson, C.: Why we cannot (yet) ensure the cyber-security of safety-critical systems. In: 24th Safety-Critical Systems Symposium, 171–182 (2016). [Online]. <http://eprints.gla.ac.uk/130822/>
- Musleh, A.S., Chen, G., Dong, Z.Y.: A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans. Smart Grid* 11(3), 2218–2234 (2019). <https://doi.org/10.1109/tsg.2019.2949998>
- Case, D.U.: Analysis of the cyber attack on the Ukrainian power grid. In: Electricity Information Sharing and Analysis Center (E-ISAC), 388, 1–29 (2016)
- Morgan, L.: Another Cyber Attack Affecting Water Supply (2021). [Online]. <https://www.cshub.com/attacks/articles/another-cyber-attack-affecting-water-supply>. Accessed on 24 Mar 2022
- Cecati, C., et al.: An overview on the smart grid concept. In: IECON 2010-36th Annual Conference on IEEE Industrial Electronics Society, pp. 3322–3327 (2010)
- Colbert, E.J., Kott, A.: Cyber-security of SCADA and Other Industrial Control Systems, vol. 66 (2016)
- Weiss, J., Weiss, J.: Protecting Industrial Control Systems from Electronic Threats. Momentum Press (2010)
- Antova, G.: Active vs. Passive Monitoring: No Longer an Either-Or Proposition (2019). [Online]. <https://www.securityweek.com/active-vs-passive-monitoring-no-longer-either-or-proposition>. Accessed on 24 Mar 2022
- Gunduz, M.Z., Das, R.: Cyber-security on smart grid: threats and potential solutions. *Comput. Network.* 169, 107094 (2020). <https://doi.org/10.1016/j.comnet.2019.107094>
- Mauriya, A., Kumar, D.: Reliability of safety-critical systems: a state-of-the-art review. *Qual. Reliab. Eng. Int.* 36(7), 2547–2568 (2020). <https://doi.org/10.1002/qre.2715>
- Mavridou, A., Papa, M.: A situational awareness architecture for the smart grid. In: Global Security, Safety and Sustainability & E-Democracy, pp. 229–236 (2011)
- Wang, W., Lu, Z.: Cyber security in the smart grid: survey and challenges. *Comput. Network.* 57(5), 1344–1371 (2013). <https://doi.org/10.1016/j.comnet.2012.12.017>
- Gupta, B.B., Akhtar, T.: A survey on smart power grid: frameworks, tools, security issues, and solutions. *Ann. Telecommun.* 72(9), 517–549 (2017). <https://doi.org/10.1007/s12243-017-0605-4>
- Franke, U., Brynielsson, J.: Cyber situational awareness—a systematic review of the literature. *Comput. Secur.* 46, 18–31 (2014). <https://doi.org/10.1016/j.cose.2014.06.008>
- Dileep, G.: A survey on smart grid technologies and applications. *Renew. Energy* 146, 2589–2625 (2020). <https://doi.org/10.1016/j.renene.2019.08.092>
- Tu, C., et al.: Big data issues in smart grid—a review. *Renew. Sustain. Energy Rev.* 79, 1099–1107 (2017). <https://doi.org/10.1016/j.rser.2017.05.134>
- Goel, N., Agarwal, M.: Smart grid networks: a state of the art review. In: 2015 International Conference on Signal Processing and Communication (ICSC), pp. 122–126 (2015)
- Mcgee, F., et al.: The state of the art in multilayer network visualization. In: Computer Graphics Forum, vol. 38, pp. 125–149 (2019)
- Yan, Y., et al.: A survey on smart grid communication infrastructures: motivations, requirements and challenges. In: IEEE Communications Surveys & Tutorials, vol. 15, pp. 5–20 (2012)
- Hurd, C.M., McCarty, M.V.: A Survey of Security Tools for the Industrial Control System Environment. Idaho National Lab. (INL), Idaho Falls, ID (United States) (2017). Tech. Rep
- Czekster, R.M.: Tools for modelling and simulating the smart grid. arXiv preprint arXiv:2011.07968, (2020)
- Samanis, E., Gardiner, J., and Rashid, A.: A taxonomy for contrasting industrial control systems asset discovery tools. arXiv preprint arXiv:2202.01604, (2022)
- Yu, E.-Y., et al.: Identifying critical nodes in temporal networks by network embedding. *Sci. Rep.* 10(1), 1–8 (2020). <https://doi.org/10.1038/s41598-020-69379-z>
- Ventresca, M., Aleman, D.: Efficiently identifying critical nodes in large complex networks. *Comput. Soc. Netw.* 2(1), 1–16 (2015). <https://doi.org/10.1186/s40649-015-0010-y>
- Yu, E.-Y., et al.: Predicting critical nodes in temporal networks by dynamic graph convolutional networks. arXiv preprint arXiv:2106.10419, (2021)
- Li, Z.-H., Duan, D.-L.: Identification of cascading dynamic critical nodes in complex networks. *Int. J. Embed. Syst.* 12(2), 226–233 (2020). <https://doi.org/10.1504/ijes.2016.10011430>
- Farzan, F., et al.: Cyber-related risk assessment and critical asset identification in power grids. In: ISGT 2014, pp. 1–5 (2014)
- Shen, Y., et al.: On the discovery of critical links and nodes for assessing network vulnerability. *IEEE/ACM Trans. Netw.* 21(3), 963–973 (2012)
- Crowder, R.: Cyber Physical systems and security. In: Electric Drives and Electromechanical Systems, pp. 271–289. Butterworth-Heinemann (2020)
- Griffor, E.R., et al.: Framework for Cyber-Physical Systems: Volume 1, Overview (2017)
- Beringer, D., Hancock, P.: Exploring situational awareness—a review and the effects of stress on rectilinear normalization (aircraft pilot performance). In: International Symposium on Aviation Psychology, 5th, pp. 646–651. Columbus (1989)
- Preden, J.: Generating situation awareness in cyber-physical systems: creation and exchange of situational information. In: Proceedings of the 2014 International Conference on Hardware/Software Codesign and System Synthesis, pp. 1–3 (2014)
- Silagy, E.: OT vs. IT: Differences, Similarities, & How They Intermix (2021). [Online]. <https://virtualarmour.com/operational-technology-vs-information-technology-differences-similarities-how-the-intermix-with-industrial-control-systems/>. Accessed on 24 Mar 2022
- Bush, S.F.: Smart Grid: Communication-Enabled Intelligence for the Electric Power Grid (2014)
- Stouffer, K., et al.: Guide to industrial control systems (ICS) security. NIST Spec. Publ. 800(82), 16 (2011)
- Pauna, A., et al.: Certification of cyber security skills of ICS/SCADA professionals. In: The European Union Agency for Network and Information Security (ENISA). Heraklion (2014)
- Liu, G., et al.: Adaptive bipartite tracking control of nonlinear multi-agent systems with input quantization. *IEEE Trans. Cybern.* 52(3), 1891–1901 (2022). <https://doi.org/10.1109/teyb.2020.2999090>

39. Liu, G., et al.: Antagonistic interaction-based bipartite consensus control for heterogeneous networked systems. *IEEE Trans. Syst. Man Cybern.: Syst.* 53(1), 71–81 (2023). <https://doi.org/10.1109/tsmc.2022.3167120>
40. ICS-ISAC: Situational Awareness Reference Architecture (SARA) (2017). [Online]. <http://ics-isac.org/blog/sara/>. accessed on 24 Mar 2022
41. Vidulich, M., et al.: Situation Awareness: Papers and Annotated Bibliography. Armstrong Lab Wright-Patterson Afb Oh Crew Systems Directorate, Tech. Rep. (1994)
42. Liu, C., et al.: Cyber risks to critical smart grid assets of industrial control systems. *Energies* 14(17), 5501 (2021). [Online]. <https://doi.org/10.3390/en14175501> <https://www.mdpi.com/1996-1073/14/17/5501>
43. Alrowaili, Y., Saxena, N., Burnap, P.: Determining asset criticality in cyber-physical smart grid. In: *Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security*, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part II 26, pp. 770–776 (2021)
44. Saxena, N., et al.: Impact evaluation of malicious control commands in cyber-physical smart grids. *IEEE Trans. Sustain. Comput.* 6(2), 208–220 (2021). <https://doi.org/10.1109/tsusc.2018.2879670>
45. Beyza, J., Garcia-Paricio, E., Yusta, J.M.: Ranking critical assets in interdependent energy transmission networks. *Elec. Power Syst. Res.* 172, 242–252 (2019). [Online]. <https://doi.org/10.1016/j.epsr.2019.03.014> <https://www.sciencedirect.com/science/article/pii/S0378779619301063>
46. Weaver, G.A., et al.: Toward a cyber-physical topology language: applications to nerc cip audit. In: *Proceedings of the First ACM Workshop on Smart Energy Grid Security*, pp. 93–104 (2013)
47. Weaver, G.A., et al.: “Cyber-physical models for power grid security analysis: 8-substation case. In: 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 140–146 (2016)
48. Wlazlo, P., et al.: A cyber topology model for the Texas 2000 synthetic electric power grid. In: *2019 Principles, Systems and Applications of IP Telecommunications (IPTComm)*, pp. 1–8 (2019)
49. Kaun, R.: What Is OT/ICS Asset Inventory and Why is it the Foundation of a Cyber Security Program? (2021). [Online]. <https://verveindustrial.com/resources/blog/what-is-ot-ics-asset-inventory-and-why-is-it-the-foundation-of-a-cyber-security-program/>. Accessed on 24 Mar 2022
50. Perelman, B.: The Role of Asset Management in ICS Network (2016). [Online]. <https://www.securityweek.com/role-asset-management-ics-network>. Accessed on 24 Mar 2022
51. Kim, K.H., et al.: Intrusion detection and identification using tree-based machine learning algorithms on dcs network in the oil refinery. *IEEE Trans. Power Syst.* 37(6), 4673–4682 (2022). <https://doi.org/10.1109/tpwrs.2022.3150084>
52. Langner: Understanding OT/ICS Asset Discovery: Passive vs. Active (2018). [Online]. <https://www.langner.com/2018/08/understanding-ot-ics-asset-discovery-passive-scanning-vs-selective-probing/>. Accessed on 24 Mar 2022
53. Blomgren, Z.: Active Network Scanning in OT Environments (2019). [Online]. <https://www.belden.com/blogs/active-network-scanning>. Accessed on 24 Mar 2022
54. Parsons, D.: ICS Defense: It's Not a “copy-Paste” from an IT Playbook (2018). [Online]. <https://www.sans.org/blog/ics-defense-its-not-a-copy-paste-from-an-it-playbook/>. Accessed on 24 Mar 2022
55. Sherry, C.: Advantages and Disadvantages of Active vs. Passive Scanning in it and OT Environments (2020). [Online]. <https://www.infosecurity-magazine.com/opinions/active-passive-scanning/>. Accessed on 24 Mar 2022
56. Langner: The Simple Truth Why ICS Detection/Passive Scanning Can't Scale (2019). [Online]. <https://www.langner.com/2019/07/the-simple-truth-why-ics-detection-passive-scanning-cant-scale/>. Accessed on 24 Mar 2022
57. WaterISAC: OT/ICS Asset Inventory – Passive Scanning vs. Selective Probing (2018). [Online]. <https://www.waterisac.org/portal/otics-asset-inventory—passive-scanning-vs-selective-probing>. Accessed on 24 Mar 2022
58. Al Ghazo, A.T., Kumar, R.: ICS/SCADA device recognition: a hybrid communication-patterns and passive-fingerprinting approach. In: *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pp. 19–24 (2019)
59. Wedgbury, A., Jones, K.: Automated asset discovery in industrial control systems-exploring the problem. In: *3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015)*, vol. 3, pp. 73–83 (2015)
60. Pospisil, O., et al.: Active scanning in the industrial control systems. In: *2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC)*, pp. 227–232 (2021)
61. Niedermaier, M., et al.: Efficient passive ICS device discovery and identification by MAC address correlation. *arXiv preprint arXiv:1904.04271*, (2019)
62. Hanka, T., et al.: Impact of active scanning tools for device discovery in industrial networks. In: *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, pp. 557–572 (2020)
63. Coffey, K., et al.: Vulnerability analysis of network scanning on SCADA systems. *Secur. Commun. Network.* 2018, 1–21 (2018). <https://doi.org/10.1155/2018/3794603>
64. Cyberx: Asset Discovery Solution Brief: How CyberX Works and How it Can Give an Opinion to Work With Active and Passive (2020). [Online]. https://cyberx-labs.com/wp-content/uploads/2018/11/CyberX_Asset_Discovery_Solution_Brief.pdf. Accessed on 24 Mar 2022
65. Tripwire: Tripwire industrial appliances TIA-2400V TIA 2800V series: security hardware for visibility and threat management. [Online]. <https://www.tripwire.com/solutions/industrial-control-systems/tripwire-industrial-appliance-datasheets> (2011). Accessed on 24 Mar 2022
66. NSAcYber: Grassmarlin: Provides Situational Awareness of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (Scada) Networks in Support of Network Security Assessments (2017). [Online]. <https://github.com/nsacyber/GRASSMARLIN>. Accessed on 22 Jun 2022
67. Splunkbase: Splunk for Asset Discovery (2013). [Online]. <https://apps.splunk.com/app/662/>. Accessed on 22 Jun 2022
68. Spiceworks: Asset Visibility for ICS Environments. [Online]. <https://www.dragos.com/platform/asset-visibility/>. Accessed on 22 Jun 2022
69. OWASP: Amass: In-Depth Attack Surface Mapping and Asset Discovery (2022). [Online]. <https://github.com/OWASP/Amass>. Accessed on 22 Jun 2022
70. Dragos Platform & Neighborhood Watch the Challenge. [Online]. https://www.dragos.com/wp-content/uploads/Dragos_CaseStudy_TrinityWaterAuthority_r5.pdf. Accessed on 22 Jun 2022
71. Tenable®: Tenable.OT. [Online]. <https://www.tenable.com/products/tenable-ot>. Accessed on 22 Jun 2022
72. Wireshark: Wireshark - Go Deep. [Online]. <https://www.wireshark.org/>. Accessed on 22 Jun 2022
73. Nmap: s7-info NSE Script. [Online]. <https://nmap.org/nsedoc/scripts/s7-info.html>. Accessed on 22 Jun 2022
74. Ayushman4: SCADA-CIP-discovery: Common Industrial Protocol Based Device Scanner over the Internet (2016). [Online]. <https://github.com/ayushman4/SCADA-CIP-Discovery>. Accessed on 22 Jun 2022
75. Ettercap: Ettercap: Ettercap Project (2020). [Online]. <https://github.com/Ettercap/ettercap>. Accessed on 22 Jun 2022
76. Verve: IT OT Asset Inventory Management. [Online]. <https://verveindustrial.com/verve-security-center/asset-inventory/>. Accessed on 22 Jun 2022
77. Dragos: CyberLens (2013). [Online]. <https://www.dragos.com/community-tools/>. Accessed on 22 Jun 2022
78. Snipe-IT: Free Open Source IT Asset Management (2022). [Online]. <https://snipeitapp.com/>. Accessed on 22 Jun 2022
79. Airbus: Airbus Asset Management Lessor Profile. [Online]. <https://centreforaviation.com/data/profiles/lessors/airbus-asset-management>. Accessed on 22 Jun 2022

80. Dragos: Sophia a Free Community Tool for Safe, Continuous, Passive Discovery of ICS Networks and Assets (2012). [Online]. <https://www.dragos.com/community-tools/>. Accessed on 22 Jun 2022
81. DragosCommunity: OT WATCH. [Online]. <https://www.dragos.com/community-tools/>. Accessed on 22 Jun 2022
82. Risk, A.: OT Asset Discovery - Applied Risk. [Online]. <https://applied-risk.com/industrial-security-services/ot-asset-discovery>. Accessed on 22 Jun 2022
83. Atimorin: SCADA-Tools (2014). [Online]. <https://github.com/atimorin/scada-tools>. Accessed on 22 Jun 2022
84. WinTECH: ModScan - Modbus Master Data Scanner (2017). [Online]. <https://www.win-tech.com/html/modbus1.htm>. Accessed on 22 Jun 2022
85. D3coder: ICS-Hunter: A Tcp Port Scanner that Specially Designed to Track Industrial Control Systems (2020). [Online]. <https://github.com/d3coder/ICS-Hunter>. Accessed on 22 Jun 2022
86. Meeas: PLCscan: Tool for Scan PLC Devices over S7comm or Modbus Protocols (2015). [Online]. <https://github.com/meeas/plcscan>. Accessed on 22 Jun 2022
87. Netresec: NetworkMiner - the NSM and Network Forensics Analysis Tool (2007). [Online]. <https://www.netresec.com/?page=NetworkMiner>. Accessed on 22 Jun 2022
88. Lansweeper: IT Asset Management Software for IT Professional. [Online]. <https://www.lansweeper.com/it-network-discovery/>. Accessed on 22 Jun 2022
89. Greenbone: Openvas-scanner (2022). [Online]. <https://github.com/greenbone/openvas-scanner>. Accessed on 22 Jun 2022
90. Axonius: Cyber Asset Inventory - Asset Management Platform. [Online]. <https://www.axonius.com/platform/asset-inventory>. Accessed on 22 Jun 2022
91. Arnaudsoullie: Modbus-scanner: Utility for Modbus/TCP (2015). [Online]. <https://github.com/arnaudsoullie/modbus-scanner>. Accessed on 22 Jun 2022
92. auconet it: BICS Asset Management. [Online]. <https://www.auconet-it.com/produkte/asset-management/?lang=en>. Accessed on 22 Jun 2022
93. Tools, P.D.: PLC Scanner (2020). [Online]. https://plcdatatools.com/demo_download/plc-scanner-software/. Accessed on 22 Jun 2022
94. ATT: USM AnywhereTM Asset Management. [Online]. <https://cybersecurity.att.com/documentation/usm-anywhere.htm?tocpath=Documentation>. Accessed on 22 Jun 2022
95. Bulw4rk: SCADA/PLC-scanner: PLC Scanner Based on SCADAS-TRANGELOVE PLCSCAN Tool (2018). [Online]. <https://github.com/bulw4rk/scadaplscanner>. Accessed on 22 Jun 2022
96. Nmap: Modbus-Discover NSE Script. [Online]. <https://nmap.org/nsedoc/scripts/modbus-discover.html>. Accessed on 22 Jun 2022
97. W3h: Icsmaster: ICS/SCADA Security Resource (2019). [Online]. <https://github.com/w3h/icsmaster>. Accessed on 22 Jun 2022
98. Lenger: Lenger Asset Management. [Online]. <https://www.lengerassetmanagement.com/>. Accessed on 22 Jun 2022
99. Nessus: Nessus ICS Asset Identification. [Online]. <https://www.tenable.com/Nessus>. Accessed on 22 Jun 2022
100. Klsecservices: s7scan: The Tool for Enumerating Siemens S7 PLCs through Tcp/ip or Llc Network (2018). [Online]. <https://github.com/klsecservices/s7scan>. Accessed on 22 Jun 2022
101. Digitalbond: Redpoint: Digital Bond's ICS Enumeration Tools (2016). [Online]. <https://github.com/digitalbond/Redpoint>. Accessed on 22 Jun 2022
102. CyberX: IoT & ICS Security. [Online]. <https://cyberx-labs.com/#the-most-mature>. Accessed on 22 Jun 2022
103. Nmap: Nmap: The Network Mapper. [Online]. <https://nmap.org/>. Accessed on 22 Jun 2022
104. Tutorial, N.: Scanning ICS/SCADA Devices (2018). [Online]. https://github.com/gnebbia/nmap_tutorial. Accessed on 22 Jun 2022
105. Awen: Dot - OT Asset, Vulnerability & Threat Vector Discovery. [Online]. <https://www.awencollective.com/dot>. Accessed on 22 Jun 2022
106. Kumari, U., Upadhyaya, S.: An interface complexity measure for component-based software systems. *Int. J. Comput. Appl.* 36(1), 46–52 (2011)
107. NCSC: Risk Management Guidance - (2018). [Online]. <https://www.ncsc.gov.uk/collection/risk-management-collection>. Accessed on 04 Aug 2022
108. Kumar, P., Ratneshwer: Some observations on dependency analysis of SOA based systems. *Int. J. Inf. Technol. Comput. Sci.* 8(1), 54–66 (2016). <https://doi.org/10.5815/ijitcs.2016.01.07>
109. Azam, M.S., et al.: A dependency model-based approach for identifying and evaluating power quality problems. *IEEE Trans. Power Deliv.* 19(3), 1154–1166 (2004). <https://doi.org/10.1109/tpwrd.2003.822537>
110. Cherdantseva, Y., et al.: A configurable dependency model of a SCADA system for goal-oriented risk assessment. *Appl. Sci.* 12(10), 4880 (2022). <https://doi.org/10.3390/app12104880>
111. Zhang, P., Peeta, S.: A generalized modeling framework to analyze interdependencies among infrastructure systems. *Transp. Res. Part B Methodol.* 45(3), 553–579 (2011). <https://doi.org/10.1016/j.trb.2010.10.001>
112. Nieuwenhuijs, A., Luijck, E., Klaver, M.: Modeling dependencies in critical infrastructures. In: *International Conference on Critical Infrastructure Protection*, pp. 205–213 (2008)
113. Ani, U., Daniel, N.C., Adewumi, S.E.: Evaluating industrial control system (ICS) security vulnerability through functional dependency analysis. *J. Comput. Sci. Appl.* 25(1), 73–89 (2018)
114. Akbarzadeh, A., Katsikas, S.: Identifying and analyzing dependencies in and among complex cyber physical systems. *Sensors* 21(5), 1685 (2021). <https://doi.org/10.3390/s21051685>
115. Hahn, A., Govindarasu, M.: Cyber attack exposure evaluation framework for the smart grid. *IEEE Trans. Smart Grid* 2(4), 835–843 (2011). <https://doi.org/10.1109/tsg.2011.2163829>
116. Wäfler, J., Heegaard, P.E.: Interdependency modeling in smart grid and the influence of ICT on dependability. In: *Meeting of the European Network of Universities and Companies in Information and Communication Engineering*, pp. 185–196 (2013)
117. Momeni, A., et al.: Mapping and modeling interdependent power, water, and gas infrastructures. In: *2018 Clemson University Power Systems Conference (PSC)*, pp. 1–8 (2018)
118. Kundur, D., et al.: Towards a framework for cyber attack impact analysis of the electric smart grid. In: *2010 First IEEE International Conference on Smart Grid Communications*, pp. 244–249 (2010)
119. Shahraeini, M., Kotzanikolaou, P.: A dependency analysis model for resilient wide area measurement systems in smart grid. *IEEE J. Sel. Area. Commun.* 38(1), 156–168 (2019). <https://doi.org/10.1109/jsac.2019.2952228>
120. He, M., Zhang, J.: A dependency graph approach for fault detection and localization towards secure smart grid. *IEEE Trans. Smart Grid* 2(2), 342–351 (2011). <https://doi.org/10.1109/tsg.2011.2129544>
121. Onwubiko, C.: Functional requirements of situational awareness in computer network security. In: *2009 IEEE International Conference on Intelligence and Security Informatics*, pp. 209–213 (2009)
122. Dillon-Merrill, P., et al.: Logic trees: fault, success, attack, event, probability, and decision trees. In: *Wiley Handbook of Science and Technology for Homeland Security* (2008)
123. Zúñiga, A.A., et al.: Classical failure modes and effects analysis in the context of smart grid cyber-physical systems. *Energies* 13(5), 1215 (2020). <https://doi.org/10.3390/en13051215>
124. Wang, Y., et al.: Computational intelligence algorithms analysis for smart grid cyber security. In: *International Conference in Swarm Intelligence*, pp. 77–84 (2010)
125. Liu, Y., et al.: A reliability assessment method of cyber physical distribution system. *Energy Proc.* 158, 2915–2921 (2019). <https://doi.org/10.1016/j.egypro.2019.01.951>
126. Vefsnmo, H., et al.: Hunting dependencies: using Bow-Tie for combined analysis of power and cyber security. In: *2020 2nd International Conference on Societal Automation (SA)*, pp. 1–8 (2021)
127. Kong, H.-K., Hong, M.K., Kim, T.-S.: Security risk assessment framework for smart car using the attack tree analysis. *J. Ambient Intell. Hum. Comput.* 9(3), 531–551 (2018). <https://doi.org/10.1007/s12652-016-0442-8>

128. Beckers, K., et al.: Determining the probability of smart grid attacks by combining attack tree and attack graph analysis. In: International Workshop on Smart Grid Security, pp. 30–47 (2014)
129. Hashemi-Dezaki, H., et al.: Risk management of smart grids based on managed charging of PHEVs and vehicle-to-grid strategy using Monte Carlo simulation. *Energy Convers. Manag.* 100, 262–276 (2015). <https://doi.org/10.1016/j.enconman.2015.05.015>
130. Wadi, M., et al.: Reliability evaluation in smart grids via modified Monte Carlo simulation method. In: 2018 7th International Conference on Renewable Energy Research and Applications (ICRERA), pp. 841–845 (2018)
131. Sorini, A., Staroswiecki, E.: Cybersecurity for the smart grid. In: *The Power Grid*, pp. 233–252 (2017)
132. Friedberg, I., et al.: STPA-SafeSec: safety and security analysis for cyber-physical systems. *J. Inf. Secur. Appl.* 34, 183–196 (2017). <https://doi.org/10.1016/j.jisa.2016.05.008>
133. Kaplan, S., Garrick, B.J.: On the quantitative definition of risk. *Risk Anal.* 1(1), 11–27 (1981). <https://doi.org/10.1111/j.1539-6924.1981.tb01350.x>
134. Voeller, J.G.: *Wiley Handbook of Science and Technology for Homeland Security*, 4 Volume Set (2010)
135. Zhou, C., et al.: Research on network security attack detection algorithm in smart grid system. In: 2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC), pp. 1407–1410 (2017)
136. Cook, A., et al.: Measuring the risk of cyber attack in industrial control systems. In: 4th International Symposium for ICS SCADA Cyber Security Research 2016 (ICS-CSR)
137. Hyder, B., Govindarasu, M.: Optimization of cybersecurity investment strategies in the smart grid using game-theory. In: 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5 (2020)
138. Shan, X.G., Zhuang, J.: A game-theoretic approach to modeling attacks and defenses of smart grids at three levels. *Reliab. Eng. Syst. Saf.* 195, 106683 (2020). <https://doi.org/10.1016/j.ress.2019.106683>
139. Anwar, F., et al.: A comprehensive insight into game theory in relevance to cyber security. *Indones. Electr. Eng. Inform.* 8(1), 189–203 (2020). <https://doi.org/10.52549/ijeiv8i1.1810>
140. Ibne Hossain, N.U., et al.: Modeling and assessing cyber resilience of smart grid using bayesian network-based approach: a system of systems problem. *J. Comput. Des. Eng.* 7(3), 352–366 (2020). <https://doi.org/10.1093/jcde/qwaa029>
141. Fenton, N., Neil, M.: *Risk Assessment and Decision Analysis with Bayesian Networks*. CRC Press, Inc (2018)
142. Holton, G.A.: Defining risk. *Financ. Anal. J.* 60(6), 19–25 (2004). <https://doi.org/10.2469/faj.v60.n6.2669>
143. Izuakor, C., White, R.: Critical infrastructure asset identification: policy, methodology and gap analysis. In: International Conference on Critical Infrastructure Protection, pp. 27–41 (2016)
144. U. S. D. of Homeland Security: National Infrastructure Protection Plan (2006)
145. Proctor, M., Smith, T.: Lessons learned from NERC CIP applied to the industrial world. In: 2017 70th Annual Conference for Protective Relay Engineers (CPRE), pp. 1–6 (2017)
146. Awati, R., Cole, B.: What Is NERC CIP (Critical Infrastructure Protection) and How Does it Work? (2022). [Online]. <https://www.techtarget.com/searchsecurity/definition/North-American-Electric-Reliability-Corporation-Critical-Infrastructure-Protection-NERC-CIP>. Accessed on 15 Sep 2022
147. Christensen, D., et al.: Risk assessment at the edge: applying NERC CIP to aggregated grid-edge resources. *Electr. J.* 32(2), 50–57 (2019). <https://doi.org/10.1016/j.tej.2019.01.018>
148. Critical infrastructure protection: Dhs list of priority assets needs to be validated and reported to congress. In: *Critical Infrastructure: Resilience and Prioritization Issues*, pp. 31–74 (2013)
149. Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP), pp. 1–19, (2012). [Online]. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm
150. Department of Defense, DoD Manual 3020.45, Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP), (2017), vol. 1. [Online]. <http://www.dtic.mil/whs/directives>
151. Ullah, S., Shetty, S., Hassanzadeh, A.: Towards modeling attacker's opportunity for improving cyber resilience in energy delivery systems. In: 2018 Resilience Week (RWS), pp. 100–107 (2018)
152. Corallo, A., Lazoi, M., Lezzi, M.: Cybersecurity in the context of industry 4.0: a structured classification of critical assets and business impacts. *Comput. Ind.* 114, 103165 (2020). <https://doi.org/10.1016/j.compind.2019.103165>
153. Crespo, A., et al.: Criticality analysis for improving maintenance, felling and pruning cycles in power lines. *IFAC-PapersOnLine* 51(11), 211–216 (2018). <https://doi.org/10.1016/j.ifacol.2018.08.262>
154. Dong, M., Li, W., Nassif, A.B.: Long-term health index prediction for power asset classes based on sequence learning. *IEEE Trans. Power Deliv.* 37(1), 197–207 (2021). <https://doi.org/10.1109/tpwr.2021.3055622>
155. Mattioli, R., Levy-Bencheton, C.: Methodologies for the Identification of Critical Information Infrastructure Assets and Services. ENISA Report (2014)
156. Alhasawi, S.: ICSrank: A Security Assessment Framework for Industrial Control Systems (ICS). Ph.D. dissertation, Liverpool John Moores University, United Kingdom (2020)
157. Haque, M.A., Shetty, S., Kamdem, G.: Improving bulk power system resilience by ranking critical nodes in the vulnerability graph. In: *Proceedings of the Annual Simulation Symposium*, pp. 1–12 (2018)
158. Goyal, A., et al.: Asset health management using predictive and prescriptive analytics for the electric power grid. *IBM J. Res. Dev.* 60(1), 4–1 (2016). <https://doi.org/10.1147/jrd.2015.2475935>
159. Li, X., et al.: Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems. *IEEE Trans. Ind. Inf.* 14(2), 608–618 (2017). <https://doi.org/10.1109/tii.2017.2740571>
160. Alvarez, D.L., et al.: A framework for asset management in electrical systems, part i: conceptual model. In: 2019 IEEE Workshop on Power Electronics and Power Quality Applications (PEPQA), pp. 1–6 (2019)
161. Prajanti, A.D., Ramli, K.: A proposed framework for ranking critical information assets in information security risk assessment using the octave allegro method with decision support system methods. In: 2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), pp. 1–4 (2019)
162. Kiss, I., Genge, B., Haller, P.: Behavior-based critical cyber asset identification in process control systems under cyber attacks. In: *Proceedings of the 2015 16th International Carpathian Control Conference (ICCC)*, pp. 196–201 (2015)
163. Martínez, L., González, V.A.V.: A novel automatic discovery system of critical assets in cyberspace-oriented military missions. In: *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1–8 (2020)
164. West, J., et al.: Automatic identification of critical digital assets. In: 2019 2nd International Conference on Data Intelligence and Security (ICDIS), pp. 219–224 (2019)
165. Park, Y., et al.: Data classification and sensitivity estimation for critical asset discovery. *IBM J. Res. Dev.* 60(4), 2–1 (2016). <https://doi.org/10.1147/jrd.2016.2557638>
166. Lasseter, R.H., Chen, Z., Pattabiraman, D.: Grid-forming inverters: a critical asset for the power grid. *IEEE J. Emer. Sel. Top. Power Electron.* 8(2), 925–935 (2019). <https://doi.org/10.1109/jestpe.2019.2959271>
167. Kure, H.I., et al.: Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Comput. Appl.* 34(1), 493–514 (2022). <https://doi.org/10.1007/s00521-021-06400-0>

168. Kure, H.I., Islam, S.: Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Phys. Syst.: Theory Appl.* 4(4), 332–340 (2019). <https://doi.org/10.1049/iet-cps.2018.5079>
169. Amin, S.M.: Smart grid: overview, issues and opportunities. *Advances and challenges in sensing, modeling, simulation, optimization and control.* *Eur. J. Control* 17(5–6), 547–567 (2011). <https://doi.org/10.3166/ejc.17.547-567>
170. Sarkar, S., et al.: Votnet: hybrid simulation of virtual operational technology network for cybersecurity assessment. In: 2018 Winter Simulation Conference (WSC), pp. 1168–1179 (2018)
171. PowerWorld: PowerWorld - the Visual Approach to Electric Power Systems (2016). [Online]. <https://www.powerworld.com/>. Accessed on 15 Apr 2022
172. Ahmed, I., et al.: A SCADA system testbed for cybersecurity and forensic research and pedagogy. In: *Proceedings of the 2nd Annual Industrial Control System Security Workshop*, pp. 1–9 (2016)
173. Alhelou, H.H., Golshan, M.E.H., Hatziaargyriou, N.D.: A decentralized functional observer based optimal LFC considering unknown inputs, uncertainties, and cyber-attacks. *IEEE Trans. Power Syst.* 34(6), 4408–4417 (2019). <https://doi.org/10.1109/tpwrs.2019.2916558>
174. SIEMENS: PSS® Power System Simulation and Modeling Software (2021). [Online]. <https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/pss-software.html>. Accessed on 14 Apr 2022
175. Ledesma, P., Gotti, D., Amaris, H.: Co-simulation platform for interconnected power systems and communication networks based on PSS/E and OMNeT++. *Comput. Electr. Eng.* 101, 108092 (2022). <https://doi.org/10.1016/j.compeleceng.2022.108092>
176. Rashed, M., et al.: State estimation in the presence of cyber attacks using distributed partition technique. In: 2020 Australasian Universities Power Engineering Conference (AUPEC), pp. 1–6 (2020)
177. MATPOWER: MATPOWER - Free, Open-Source Tools for Electric Power System Simulation and Optimization (2019). [Online]. <https://matpower.org/>. Accessed on 18 Apr 2022
178. Che, L., Liu, X., and Li, Z.: Fast screening of high-risk lines under false data injection attacks. *IEEE Trans. Smart Grid*, 10 (4), 4003–4014, <https://doi.org/10.1109/tsg.2018.2848256>, (2018)
179. Pan, K., et al.: Co-simulation for cyber security analysis: data attacks against energy management system. In: 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 253–258 (2017)
180. DigSILENT: PowerFactory - DiGSILENT (2019). [Online] p. na. <https://www.digsilent.de/en/powerfactory.html>. Accessed on 14 Apr 2022
181. Findrik, M., et al.: Towards secure and resilient networked power distribution grids: process and tool adoption. In: 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 435–440 (2016)
182. Hammad, E., Ezeme, M., Farraj, A.: Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification. *Int. J. Electr. Power Energy Syst.* 104, 817–826 (2019). <https://doi.org/10.1016/j.jepes.2018.07.058>
183. PSCAD: Overview | PSCAD/EMTDC Power Systems Simulation (2021). [Online]. <https://www.pscad.com/software/pscad/overview>. Accessed on 18 Apr 2022
184. Lingaraju, K., et al.: Simulation of the effect of false data injection attacks on SCADA using PSCAD/EMTDC. In: 2020 52nd North American Power Symposium (NAPS), pp. 1–5 (2021)
185. Krishnamurthy, D.: psst: an open-source power system simulation toolbox in python. In: 2016 North American Power Symposium (NAPS), pp. 1–6 (2016)
186. OpenDSS: OpenDSS - Electric Power Distribution System Simulator (1997). [Online]. <http://sourceforge.net/projects/electricdss/>. Accessed on 18 Apr 2022
187. Etap: Power Monitoring and Simulation Software | Power Management System. [Online]. <https://etap.com/packages/monitoring-simulation>. Accessed on 14 Apr 2022
188. HOMER Energy: HOMER Pro - Microgrid Software for Designing Optimized Hybrid Microgrids (2018). [Online]. <https://www.homerenergy.com/products/pro/index.html>. Accessed on 14 Apr 2022
189. Thurner, L., et al.: pandapower—an open-source python tool for convenient modeling, analysis, and optimization of electric power systems. *IEEE Trans. Power Syst.* 33(6), 6510–6521 (2018). <https://doi.org/10.1109/tpwrs.2018.2829021>
190. Guironnet, A., et al.: Towards an open-source solution using modelica for time-domain simulation of power systems. In: 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pp. 1–6 (2018)
191. Larsson, M.: Objectstab—an educational tool for power system stability studies. *IEEE Trans. Power Syst.* 19(1), 56–63 (2004). <https://doi.org/10.1109/tpwrs.2003.821001>
192. Antoine, J., Stubbe, M.: EUROSTAG, software for the simulation of power system dynamics. its application to the study of a voltage collapse scenario. In: *IEEE Colloquium on Interactive Graphic Power System Analysis Programs*, pp. 1–4 (1992)
193. EMTP: EMTP Power Simulator. [Online]. <https://www.emtp.com/products/emtp>. Accessed on 14 Apr 2022
194. GE Energy Consulting: PSLE | Transmission Planning Software | GE Energy Consulting. [Online]. <https://www.geenergyconsulting.com/practice-area/software-products/pslf>. Accessed on 25 Apr 2022
195. Jahromi, M.Z., et al.: Cybersecurity enhancement of transformer differential protection using machine learning. In: 2020 IEEE Power & Energy Society General Meeting (PESGM), pp. 1–5 (2020)
196. Opal-RT Technologies Inc.: RT-LAB OPAL-RT Technologies. Tech. Rep. (2020). [Online]. <https://www.opal-rt.com/contact-technical-support/>
197. Chlela, M., et al.: Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks. In: 2016 IEEE Power and Energy Society General Meeting (PESGM), pp. 1–5 (2016)
198. Sarikan, A., Aydemir, M.T.: Real time digital simulation (RTDS) software and hardware in the loop (HIL) architecture for brushless DC motors. In: *Melecon 2010-2010 15th IEEE Mediterranean Electro-technical Conference*, pp. 779–783 (2010)
199. Razaq, A., et al.: Simulating smart grid: Co-simulation of power and communication network. In: 2015 50th International Universities Power Engineering Conference (UPEC), pp. 1–6 (2015)
200. Ns-3: ns-3 | a Discrete-Event Network Simulator for Internet Systems (2021). [Online]. <https://www.nsnam.org/>. Accessed on 14 Apr 2022
201. Terruggia, R., Dondossola, G.: Cyber security analysis of smart grid communications with a network simulator. In: *DA-CH Conference on Energy Informatics*, pp. 153–164 (2015)
202. OMNeT++ Discrete Event Simulator (2002). [Online]. <https://omnetpp.org/https://omnetpp.org/>. Accessed on 14 Apr 2022
203. Asri, S., Pranggono, B.: Impact of distributed denial-of-service attack on advanced metering infrastructure. *Wireless Pers. Commun.* 83(3), 2211–2223 (2015). <https://doi.org/10.1007/s11277-015-2510-3>
204. NeSSI2: Network Security Simulator (2015). [Online]. <http://www.nessi2.de/>. Accessed on 18 Apr 2022
205. Jha, A.V., et al.: A comprehensive risk assessment framework for synchrophasor communication networks in a smart grid cyber physical system with a case study. *Energies* 14(12), 3428 (2021). <https://doi.org/10.3390/en14123428>
206. S. N. T. Inc.: QualNet - Network Simulation (2019). [Online]. <https://www.scalable-networks.com/products/qualnet-network-simulation-software>. Accessed on 18 Apr 2022
207. Jha, A.V., et al.: Analytical design of synchrophasor communication networks with resiliency analysis framework for smart grid. *Sustainability* 14(22), 15450 (2022). <https://doi.org/10.3390/su142215450>

208. Chen, B., et al.: Implementing a real-time cyber-physical system test bed in RTDS and OPNET. In: 2014 North American Power Symposium (NAPS), pp. 1–6 (2014)
209. OPNET: OPNET Network Simulator - Opnet Projects (2012). [Online]. <https://opnetprojects.com/opnet-network-simulator/>. Accessed 14 Apr 2022
210. Mugombozi, C.F., et al.: Collaborative simulation of heterogeneous components as a means toward a more comprehensive analysis of smart grids. In: 2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), pp. 1–6 (2019)
211. SCADABR: ScadaBR: instaladores do ScadaBR para Windows e Linux. ScadaBR - Open source Free SCADA (2021). [Online]. <https://github.com/ScadaBR/ScadaBR>. Accessed on 14 Apr 2022
212. OpenSCADA: Open SCADA Project (2006). [Online]. <http://oscada.org/>. Accessed on 14 Apr 2022
213. Cmu-sei: SCADASim: The SCADA Simulator (2021). [Online]. <https://github.com/cmu-sei/SCADASim>. Accessed on 14 Apr 2022
214. Alves, T.: The OpenPLC Project | openplcproject.Com. [Online]. <https://www.openplcproject.com/>. Accessed on 14 Apr 2022
215. Mets, K., Ojea, J.A., Develder, C.: Combining power and communication network simulation for cost-effective smart grid analysis. *IEEE Commun. Surv. Tutor.* 16(3), 1771–1796 (2014). <https://doi.org/10.1109/surv.2014.021414.00116>
216. Hopkinson, K., et al.: EPOCHS: a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. *IEEE Trans. Power Syst.* 21(2), 548–558 (2006). <https://doi.org/10.1109/tpwrs.2006.873129>
217. Lin, H., et al.: GECON: global event-driven co-simulation framework for interconnected power system and communication network. *IEEE Trans. Smart Grid* 3(3), 1444–1456 (2012). <https://doi.org/10.1109/tsg.2012.2191805>
218. Queiroz, C., Mahmood, A., Tari, Z.: SCADASim—a framework for building SCADA simulations. *IEEE Trans. Smart Grid* 2(4), 589–597 (2011). <https://doi.org/10.1109/tsg.2011.2162432>
219. Lévesque, M., et al.: Communications and power distribution network co-simulation for multidisciplinary smart grid experimentations. In: Proceedings of the 45th Annual Simulation Symposium, pp. 1–7 (2012)
220. Liberatore, V., Al-Hammouri, A.: Smart grid communication and co-simulation. *IEEE 2011 EnergyTech*, 1–5 (2011)
221. Wermann, A.G., et al.: ASTORIA: a framework for attack simulation and evaluation in smart grids. In: NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium, pp. 273–280 (2016)
222. Saxena, N., et al.: CPSA: a cyber-physical security assessment tool for situational awareness in smart grid. In: Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and Privacy, pp. 69–79 (2017)
223. Sadnan, R., et al.: Distributed optimization for power distribution systems with cyber-physical co-simulation. In: 2021 IEEE Power & Energy Society General Meeting (PESGM), pp. 1–5 (2021)
224. Awad, A., Bazan, P., German, R.: SGsim: a simulation framework for smart grid applications. In: 2014 IEEE International Energy Conference (ENERGYCON), pp. 730–736 (2014)
225. Anderson, K., et al.: GridSpice: a distributed simulation platform for the smart grid. *IEEE Trans. Ind. Inf.* 10(4), 2354–2363 (2014). <https://doi.org/10.1109/tii.2014.2332115>
226. Pan, Z., et al.: NS3-MATLAB co-simulator for cyber-physical systems in smart grid. In: 2016 35th Chinese Control Conference (CCC), pp. 9831–9836 (2016)
227. De Souza, E., Ardakanian, O., Nikolaidis, I.: A co-simulation platform for evaluating cyber security and control applications in the smart grid. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1–7 (2020)
228. Ni, M., et al.: A cyber physical power system co-simulation platform. In: 2018 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), pp. 1–5 (2018)
229. Amarasekara, B., et al.: Co-simulation platform for smart grid applications. In: 2015 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA), pp. 1–6 (2015)
230. Le, T.D., et al.: Gridattacksim: a cyber attack simulation framework for smart grids. *Electronics* 9(8), 1218 (2020). <https://doi.org/10.3390/electronics9081218>
231. Huang, R., et al.: Open-source framework for power system transmission and distribution dynamics co-simulation. *IET Gener. Transm. Distrib.* 11(12), 3152–3162 (2017). <https://doi.org/10.1049/iet-gtd.2016.1556>
232. Al-Hammouri, A.T.: A comprehensive co-simulation platform for cyber-physical systems. *Comput. Commun.* 36(1), 8–19 (2012). <https://doi.org/10.1016/j.comcom.2012.01.003>
233. Mallouhi, M., et al.: A testbed for analyzing security of SCADA control systems (TASSCS). In: ISGT 2011, pp. 1–7 (2011)
234. GMLC: Hierarchical Engine for Large-Scale Infrastructure Co-simulation (HELICS). [Online]. <https://helics.org/>. accessed on 25 Apr 2022
235. Georg, H., et al.: INSPIRE: integrated co-simulation of power and ICT systems for real-time evaluation. In: 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 576–581 (2013)
236. Sun, X., et al.: A co-simulation platform for smart grid considering interaction between information and power systems. In: ISGT 2014, pp. 1–6 (2014)
237. van der Meer, A., et al.: Cyber-physical energy systems modeling, test specification, and co-simulation based testing. In: 2017 IEEE Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), pp. 1–9 (2017)
238. Chinnow, J., et al.: A simulation framework for smart meter security evaluation. In: 2011 IEEE International Conference on Smart Measurements of Future Grids (SMFG) Proceedings, pp. 1–9 (2011)

How to cite this article: Alrowaili, Y., et al.: A review: Monitoring situational awareness of smart grid cyber-physical systems and critical asset identification. *IET Cyber-Phys. Syst., Theory Appl.* 1–26 (2023). <https://doi.org/10.1049/cps2.12059>